# Library of Congress
## Law Library of Congress



# Online Privacy Law: United Kingdom

Research & Reports | Guide to Law Online | Legal Research Guides | **Legal Topics** | Guides to Our Collections
Back to Online Privacy Law

*A 2017 updated version of this report is available



*Data protection legislation in the UK is primarily based upon Directives from the European Union. It aims to protect the rights of individuals to ensure that their personal information remains private and secure. It provides individuals with a number of rights, including a right to access information and correct any errors. The Information Commissioner has an active role in educating the public and organizations about the data protection legislation, assisting data subjects in enforcing their rights, and imposing sanctions and enforcement actions against those who breach the legislation. The Information Commissioner's role as enforcer has been strengthened, with increased penalties available for cases of egregious breaches of the laws.*

## I. Legal Framework

The United Kingdom does not have a written constitution that enshrines a right to privacy for individuals and there is no common law that provides for a general right to privacy. The UK has, however, incorporated the European Convention on Human Rights into its national law, which provides for a limited right of respect towards an individual's privacy and family life.[1] The primary legislation in the UK that regulates the holding of an individual's personal data by companies, and consequently has an impact on information concerning the private lives of individuals, is the Data Protection Act 1998 (DPA).[2] The Information Commissioner has stated that the aim of the DPA is "to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information."[3]

### A. Data Protection Act 1998

The DPA was enacted and implemented to meet the requirements of the European Union's Data Protection Directive 95/46/EC. Although the DPA implements the Data Protection Directive, which refers expressly to privacy, the DPA does not mention the word privacy in any of its provisions.[4]

The DPA regulates the processing of personal information of individuals. It is broad and applies to obtaining, holding, using or disclosing this personal information.[5] Following implementation of the DPA, the Deputy Data Protection Registrar noted that

> if the 1998 Act satisfies the Directive, then it serves to protect the rights of individuals to privacy, as at least in respect of the processing of personal data . . . . I do not assert that data protection legislation is comprehensive privacy legislation protecting every aspect of that right, but I do ask how it can be doubted that, as a matter of law, data protection is a form of privacy protection.[6]

While the DPA is a relatively recent piece of legislation largely based on the requirements of the European Union Directive, its origin can be seen in the 1960s, and the Younger Committee on Privacy. This Committee was established amid growing concern over the amount of personal data held by organizations to which individuals had no right of access. The terms of reference of the Committee

was to "consider whether legislation is needed to give further protection to the individual citizen and to commercial and industrial interests against intrusion into privacy by private persons and organisations and companies."[7] While the committee did not see a need for the legislation at the time, it did formulate ten principles for good data management. These principles have continued to be in use since their formation and have been the staple of data protection legislation in the UK.

Schedule 1 of the DPA contains eight principles that regulate how personal data should be handled, which are "based on the premise of compliance with principles of good data management."[8] These principles apply to both online and offline data and require that

- Personal data shall be processed fairly[9] and lawfully and, in particular, shall not be processed unless
  - At least one of the conditions in Schedule 2 is met, and
  - In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.[10]

"Personal data" is defined as data that "relate to a living individual who can be identified—(a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller."[11] In the leading case on the interpretation of "personal data," the Court of Appeal interpreted the term narrowly. It considered the fact that data may be associated with an individual's name was not sufficient to make it personal. Two additional factors are required: that the information should be "biographical in a significant sense,"[12] and that the data should not include a merely incidental reference to the data subject. The information must affect the data subject's "privacy, whether in his person or family life, business or professional capacity."[13]

The DPA applies to individuals and entities that are established in the UK and that process data in the context of the establishment.[14] The law regards those that are ordinarily resident in the UK as established in the country. There are a number of means under which various entities are or may be ordinarily resident in the UK. Corporate bodies are considered to be ordinarily resident and thus established in the UK if they are incorporated under UK law. Partnerships and other unincorporated associations are treated as being established in the UK if they are either formed under UK law or maintain a regular practice, office branch, or agency through which they conduct activities in the UK.[15] A "branch" in this instance refers to the "term used in Community law for an organizational sub-division of a company which has some degree of both identity and independence."[16]

Back to Top

## II. Current Law

### A. The Collection, Storage, and Use of Personal Data by Online Media or Services

While the DPA accords data subjects certain rights over their personal data, these rights do not absolutely prohibit a company from collecting data about them. The collection, storage, and use of personal data by online media or services is permitted, within the constraints of the DPA. The Information Commissioner has noted that it is bad practice to require a name and email from someone simply to allow them to view a website.[17] Further information obtained about data subjects through online services, particularly through cookies, is regulated through the Privacy and Electronic Communications (EC Directive) Regulations 2003, as amended, which implemented European Directives 2002/58/EC[18] and 2009/136/EC[19] into the national law of the UK.[20] This regulation provides that

> 6.—(1) Subject to paragraph (4), a person shall not use an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.

(2) The requirements are that the subscriber or user of that terminal equipment—

(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

(b) is given the opportunity to refuse the storage of or access to that information.[21]

**B. Other Means of Regulating Data Activity**

The DPA regulates the collection, storage, and use of personal data by both offline and online media or services. Data subjects' rights include a right of access to personal data held about them, the right to have this information corrected if it is wrong, and the right to stop personal data from being used for the purposes of direct marketing.[22]

**C. Retention of Data**

The laws governing the retention of data by Internet Service Providers (ISPs) are contained in the Data Protection Act 1998;[23] the Privacy and Electronic Communications (EC Directive) Regulations 2003;[24] and the Anti-terrorism, Crime and Security Act 2001, [25] along with its Code of Practice.[26]

The retention of data by ISPs for the purpose of national security was initially governed by the Anti-terrorism, Crime and Security Act 2001. This Act required the Secretary of State to establish what was initially a voluntary Code of Practice in relation to the retention of communications data that was approved by Houses of Parliament prior to coming into force.[27] The Act required that the Code of Practice contain any provisions necessary for the purposes of safeguarding national security, preventing or detecting crime, or prosecuting offenders.[28] As the Code was voluntary, a breach of any of its provisions did not lead to criminal or civil sanctions; however, if the Secretary of State felt that the voluntary Code of Practice was ineffective, he had authority to impose mandatory retention orders on ISPs, although these required the approval of both Houses of Parliament.[29]

The Data Retention (EC Directive) Regulations 2009[30] replaced this voluntary regime and imposed a statutory requirement on public communications providers to retain data that is necessary to trace and identify the source, destination, type, date, time, and duration of a communication for all types of communications (fixed telephone lines, mobile phones, and Internet communications). For cell phones, communications providers must also retain data necessary to identify the user's communications equipment and the data required to identify the location of the equipment. For communications conducted via the Internet, the communications provider must also retain information relating to the user's communication equipment.[31]

1. Types of Data to Be Retained

A Code of Practice issued under the DPA provides that if a business has personal information that it does not use, that information should no longer be collected and any existing data should be deleted.[32] The Information Commissioner recommends that if data can be stored without identifying information, then this should be done. For example, it recommends that the last eight numbers of an IP address be removed, or the last identifying numbers of a postal code.[33] Data subjects have a right under the DPA to request that any personal information held on them be deleted. The Information Commissioner recommends that this occur unless there are other legal obligations to retain the data.[34]

2. Amount of Time Data Must Be Retained

The Data Retention (EC Directive) Regulations 2009[35] sets forth specific requirements for the retention of communications data with regard to both landline telephones, mobile telephones, and Internet access, and email or Internet phones. This regulation moved the UK away from a voluntary regime of communications data retention to a mandatory system. The intention was that creating certainty by retaining this data for a set period of time would enable law enforcement to build stronger cases and prevent serious offenses before they occur.[36] This regulation provides that the communications data associated with these forms should be retained for a period of twelve months.[37]

3. The Cost of Retention

The Data Retention (EC Directive) Regulations 2009 provides that the Secretary of State may reimburse public communications providers for any costs incurred in complying with the requirements of the Regulations.[38]

**D. Transparency**

One of the primary purposes of the DPA is to make sure that data subjects are aware of how information collected about them will be used.[39] This information should be contained in the sites' privacy notice. The Code states that this notice should "[have] sufficient prominence for people to access it easily. It should be written in a way that the people who access your service are likely to understand. It should use font sizes and colours that make the text easy to read."[40]

As noted above, the Privacy and Electronic Communications Regulations 2003 provide that

(1) Subject to [the exceptions noted below], a person shall not use an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a subscriber or user unless the

requirements of paragraph (2) are met.

(2) The requirements are that the subscriber or user of that terminal equipment—

(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

(b) is given the opportunity to refuse the storage of or access to that information.[41]

While the statute is drafted broadly, this provision predominantly applies to the use of cookies for online users. The data subject must be made aware that the cookies are there and of what the cookies are doing, and must provide consent for the cookies to be placed on his/her computer.[42] There are two exceptions to this rule for situations where the cookie is "(a) for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network; or (b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user."[43]

The DPA provides that data subjects may, by written notice, require the data controller to stop, or not begin, to process their personal data if it will or is likely to cause unwarranted substantial damage or substantial distress to the data subject or another person.[44]

### E. Special Safeguards for Personal Data

When questioned about companies' policies concerning harvesting and retaining personal data from users, the ICO stated that one of the Data Protection requirements is that UK companies must be "open and up front" with any users about how, and for what purposes, their personal data will be used.[45]

### F. Safeguards Against Data Collection by Smartphone Applications

There is no current law specific to smartphones. The collection of data by smartphone applications is subject to the same data protection requirements as other online services.

### G. Limits on Geo Data

Geo data (known as "location data" in the UK) may only be processed if the subscriber or user cannot be identified from the data.[46] If the service provider has the data subject's consent, it may process geo data "where it is necessary to provide a value-added service."[47] There is no prescribed form as to how the consent should be obtained;[48] however, the data subject must have information on "(a) the types of location data that will be processed; (b) the purposes and duration of the processing of those data; and (c) whether the data will be transmitted to a third party for the purpose of providing the value-added service."[49]

The ICO provides guidance that the data subject "should be given enough clear information for them to have a broad appreciation of how the data is going to be used and the consequences of consenting to such use."[50] Once the data subject has provided consent, he or she has the opportunity to withdraw it at any point in time.[51]

### H. Protection of Minors and Facebook

The Department for Education supports the UK's Council for Child Internet Safety (UKCCIS), a voluntary organization that works to protect children from online risks, such as cyberbullying, accessing harmful or inappropriate information (e.g., suicide information or pro- anorexia sites), sexual predators, and scams.[52] The UKCCIS promotes Internet safety for children through both education and industry guidelines. The education element includes a behavioral code entitled "click clever click safe." This code "encourage[s] children to keep personal information safe; avoid opening links and emails from unknown senders; and tell someone they trust if they encounter anything online that upsets them."[53]

The use of social media among children has exploded: 43% of nine- to twelve-year-olds across the UK have a profile on a social networking site. One in three has a Facebook account, despite the minimum age set by the company to join being thirteen. One quarter of these nine- to twelve-year-olds do not use privacy restrictions on their Facebook profile, and one-fifth of these publicly display their address and/or phone number. A study into the use of social media by children has noted that "[m]any providers try to restrict their users to 13-year-olds and above but we can see that this is not effective. Especially younger children are less likely to use privacy options and to understand the safety features that are available."[54] During a conference on children and the UK media in 2012, Facebook informed delegates that they were "unable to prevent children under 13 setting up Facebook accounts, despite this being against government policy."[55]

Many schools across the UK have issued guidance notes on how to address online bullying conducted through Facebook. The guidance particularly focuses on those under the age of thirteen. The main measure taken is that the site is routinely blocked by filters at schools. In cases where bullying arises through Facebook outside of school and spills over into school hours, the general policy is to contact Facebook to request the removal of these accounts if the children involved are under the age of thirteen.[56]

### I. Technical and Organizational Security Measures

Principle seven of the DPA requires that

> [a]ppropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.[57]

Guidance on the level of security to be taken is provided in the DPA, but is rather general:

> Having regard to the state of technological development and the cost of implementing any measures, the measures [taken] must ensure a level of security appropriate to—(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and (b) the nature of the data to be protected.[58]

These requirements apply, even if the processing of data is outsourced.[59] The ICO currently expects the minimum standard of adequate security to be encryption.[60]

### J. User Anonymity

The DPA does not require online services to allow users to remain anonymous. The Privacy and Electronic Communications (EC Directive) Regulations 2003 provides that users should have the opportunity to refuse to use cookies, to help enable them to remain anonymous; however, "it does not specify whose wishes should take precedence if they are different."[61]

### K. Data Protection Agencies

The Agency responsible for overseeing the implementation of the Data Protection Act in the UK is the Information Commissioner's Office (the ICO). The functions of the ICO include monitoring practices of the online media and service providers, imposing sanctions, educating the public as well as assisting data subjects enforcing their rights provided for under the DPA.[62] Further information about the ICO is provided below.

### L. Rights and Remedies for Users

The DPA provides data subjects with seven rights under its provisions:

1. The right to subject access (discussed below)
2. The right to prevent processing
3. The right to prevent processing for direct marketing
4. Rights in relation to automated decision making
5. The right to compensation
6. The right to rectification, blocking, erasure and destruction
7. The right to ask the Commissioner to assess whether the Act has been contravened[63]

If requested by a data subject who feels that his/her personal information has not been processed in accordance with the provisions of the DPA, the ICO may make an assessment of compliance. If this assessment determines that the DPA has been breached, the ICO may serve an enforcement notice on the data controller.[64]

### M. Subject Access

Pursuant to section 7 of the DPA, a data subject in the UK has a right of access to personal data, and data controllers must respond within forty days of receiving the data subject's request for such access.[65] When accessing data, the DPA allows the data controller to impose a fee, typically £10 (approximately US$15), on the data subject requesting the access. However, the Code of Practice provides that it is good practice not to impose this fee if the data controller does not incur any additional costs.[66]

The right provided by section 7 is not unfettered. As stated by the court, it is "not an automatic key to any information, readily accessible or not, of matters in which [the data subject] may be named or involved."[67]

Section 7 of the DPA provides that the data subject may be informed whether any personal data that he/she is the subject of is being processed by or on behalf of the data collector. If the data controller holds personal data relating to the data subject, the data controller is required to provide the data subject with

> (i) the personal data of which that individual is the data subject, (ii) the purposes for which they are being or are to be processed, and (iii) the recipients or classes of recipients to whom they are or may be disclosed.[68]

The data controller must also provide the data subject with the source of this data and, if the data is processed automatically for the purposes of evaluating matters relating to the data subject (i.e., the subject's creditworthiness), the data controller must inform the data subject of "the logic involved in that decision-taking."[69]

There are some exemptions to providing information in response to a subject access request. If providing a copy of the data involves a disproportionate effort, the data controller is exempt from the requirements contained in section 7.[70] If the information that the data controller holds also relates to an identifiable third party, the data controller is under no obligation to disclose the information unless the third party consents, or it is "reasonable in all the circumstances to comply with the request without the consent of the other individual."[71]

Cases interpreting this section have ruled that it simply provides the data subject with a right to know whether his/her personal data is being processed, the purposes for this, and to whom this data is being disclosed.[72] While there is a statutory right for the data subject to receive "information constituting any personal data of which that individual is the data subject,"[73] the case law provides that this right is not "coterminous with a right to disclosure of documents."[74] The duty of data controllers to conduct searches for the personal data of the data subject has also been considered before the court. For this issue, the court found that certain data controllers could receive voluminous requests that imposed a large burden. As a result, the court held that the duty of the data controller is to make a "reasonable and proportionate search" in response to a subject access request.[75] This judgment has been criticized with regard to the "reasonable and proportionate" search limit; however, one commentator has noted that while this judgment narrowed down the responsibilities of the data controller it would be "illogical for proportionality to only apply to the supply of a copy of the data, when the real difficulty and expense is in locating, retrieving and collating the information in the first place."[76]

The DPA contains a number of exemptions to the types of personal data that may be requested.[77] These exemptions generally mirror those contained in the Data Protection Directive, such as information to be used for the purposes of the prevention or detection of crime, national security, crime prevention, or journalism. The DPA does contain some additional exemptions that are specific to it. These include data relating to the preparation of confidential references, the armed forces, Crown employment, negotiations, corporate finance, examination scripts, management forecasts, a legal professional privilege, or self- incrimination.[78]

If a data controller refuses to comply with a subject access request, the applicant may make a complaint to the Information Commissioner, or apply to the Court for an order to compel the controller to disclose the information. Under the DPA, if the court is satisfied that the data controller has not met its obligations under the Act, it can order the data controller to comply with the request. [79]

### N. Right to Prevent Processing

In accordance with the Data Protection Directive, the DPA includes the right to prevent the processing of data that is likely to cause damage or distress, that will be used for the purposes of direct marketing, or in relation to automated decision making.[80] In the case of *Roberson v. Wakefield Metropolitan District Council*, a data subject wished to have his name withheld from the electoral register, as the information on the register was sold for direct marketing purposes. The electoral registration officer refused to comply with the request, noting that electors were required to complete certain forms and be listed on the register in order to be able to lawfully vote. The court found for the complainant and held that "the legal rules concerning representation of the people must be construed in a manner which is Directive compliant and consistent with the Data Protection Act 1998."[81] As a result of this judgment, the electoral register is now in two parts, one that allows data subjects to opt out of direct marketing, and a second register that is open.

To exert the right to prevent the processing of data in these circumstances the data subject must apply to court and, in certain cases, may be able to obtain compensation. In cases where the information is inaccurate, the court has the power to order the correction, blocking, erasure, or destruction of the relevant data.[82]

### O. Sanctions

The ICO has stated that its "aim is to ensure organisations comply with the law."[83] If an organization fails, or refuses to comply voluntarily with the DPA, the ICO has a range of both criminal and administrative sanctions at its disposal. These sanctions have been strengthened over the past few years. For example, in 2008, through the Criminal Justice and Immigration Act,[84] the Information Commissioner was provided with the authority to serve a monetary penalty notice on data controllers in certain circumstances.

The sanctions available to the ICO include the following:

- **Information notice:** this requires organisations to provide the Information Commissioner with specified information within a certain time period.
- **Undertaking:** this commits an organisation to a particular course of action in order to improve its compliance.
- **Enforcement notice:**[85] this compels an organisation to take the action specified in the notice to bring about compliance with the Regulations. For example, a notice may be served to compel an organisation to start gaining consent for cookies. Failure to comply with an enforcement notice can be a criminal offence.
- **Monetary penalty notice:** a monetary penalty notice requires an organisation to pay a monetary penalty of an amount determined by the ICO, up to a maximum of £500,000. This power can be used in the most serious of cases.[86]

Under revised regulations, public electronic communications service providers must notify the ICO if a personal data breach occurs. A personal data breach is defined as

> a breach of security leading the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provisions of a public electronic communications service.[87]

Under the Privacy and Electronic Communications (EC Directive) Regulations, if a service provider fails to notify the Information Commissioner of a breach of security the ICO has the authority to issue a fixed monetary penalty of £1,000 (approximately US$1,600).[88] In cases of serious contraventions of the Privacy and Electronic Communications Regulation that are deliberate, or where the person responsible for preventing the contravention fails to take reasonable steps to prevent it, and where the breach is likely to cause substantial damage or distress, the ICO has the authority to impose a higher civil monetary penalty. This penalty may be a fine of up to £500,000 (approximately US$700,000).[89]

### P. Criminal Offenses

While breaching the data protection principles alone is not a criminal offense, it may give rise to claims for compensation from data subjects that have suffered damage and distress, or the imposition of a financial penalty from the ICO. There are a number of criminal offenses contained within the DPA. The ICO has the authority to bring criminal proceedings in relation to these offenses. The offenses are generally strict liability regulatory offenses. The most important offenses with regard to data subjects involve obtaining personal data without authorization.[90] These offenses relate to knowingly or recklessly obtaining, disclosing, or procuring disclosure, where there is a risk that the DPA would be contravened. This contravention requires the offending party to have failed to take reasonable steps to prevent the contravention, with this breach being likely to cause substantial damage or distress to the party whose data has been compromised.[91] If a person to whom the DPA applies knowingly or recklessly discloses or obtains personal data, he or she is guilty of an offense and subject to a fine. The court can also order the forfeiture, destruction, or erasure of any information that appears to have been used in the commission of an offense under the DPA.[92]

Criminal offenses created by the DPA include

- unlawfully obtaining, disclosing, or procuring the disclosure of personal data;
- selling, or offering to sell, personal data which has been unlawfully obtained;
- processing personal data without notifying the Information Commissioner (and other offences related to notification);
- failing to comply with an enforcement notice or an information notice, or knowingly or recklessly making a false statement in compliance with an information notice;
- obstructing, or failing to give reasonable assistance in, the execution of a search warrant;
- requiring someone, for example during the recruitment process, to exercise their subject access rights to supply certain information (such as records of their criminal convictions), which the person wanting it would not otherwise be entitled to. This offence, known as “enforced subject access”, is not yet in force; and
- the unlawful disclosure of certain information by the Information Commissioner, his staff or agents.[93]

Individuals that are in management roles within a corporation or company may be personally guilty of an offense as well as the corporate body if “the offence was committed with their consent or connivance; or the offence is attributable to neglect on their part.”[94]

As noted above, actions for offenses under the DPA are typically brought by the Information Commissioner. If the case is heard in the magistrates’ court a fine of up to £5,000 (approximately US$7,000) may be imposed. This rises to an unlimited amount if the case is tried on indictment and heard by the Crown Court.[95]

### Q. Application of the Data Protection Act to Transborder Data Flows

The Eighth Data Protection Principle prohibits the transfer of personal data outside of the European Economic Area (EEA) (“transborder data flow”), unless the recipient country either has an adequate level of personal data protection or the transfer falls within an exception or derogation. Specifically, the DPA provides that

> [p]ersonal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.[96]

In order to lawfully transfer personal data outside of the EEA in compliance with the DPA to a company in a country that does not have laws considered to be adequate, it must meet one of the exemptions or derogations contained in the DPA.[97]

The derogations to the DPA that permit the transfer of personal data to third countries considered to have inadequate levels of protection arise where the

- data subject has provided his/her consent for the transfer;
- transfer is necessary for the performance or conclusion of a contract between the data subject and data controller that is entered to at the request or is in the interests of the data subject;
- transfer is necessary for reasons of substantial public interest;

- transfer is necessary for the purpose of, or in connection with, any legal proceedings; or is necessary to obtain legal advice or for defending legal rights;
- transfer is necessary to protect the vital interests of the data subject;
- transfer is of part of personal data on a public register and all conditions regarding the register are complied with; or
- transfer is made on terms that are of a kind approved by the Commissioner ensuring that data subjects have adequate safeguards, rights, and freedoms.[98]

If any of these derogations are met, personal data that falls within the scope of the DPA may be lawfully transferred outside of the EEA.

Back to Top

## III. Role of Data Protection Agencies

The UK's Information Commissioner's Office (ICO) was established as the "independent authority . . . to uphold information rights in the public interest . . . and data privacy for individuals."[99] The ICO received its name in 2001, when it replaced the Data Protection Commissioner, as the office was given the additional responsibility of handling issues under the Freedom of Information Act.[100] The original office of Data Protection Registrar was established in 1984 in response to the enactment of the Data Protection Act 1984.[101]

The ICO currently has a staff of over 350 people and a budget of almost £20 million (approximately US$32 million). The ICO has received over 26,000 cases relating to data protection and closes 42% of those cases within thirty days.[102] In terms of enforcement actions, the ICO has completed forty-six undertakings and five prosecutions, and imposed four civil monetary penalties, over the past year.[103]

The ICO is responsible for promoting good practice and observance of the DPA by datacontrollers, producing codes of practice, reporting to Parliament on the operation of the DPA, and providing assistance to data subjects who are bringing proceedings under some provisions of the DPA.[104]

### A. Functions of the ICO

1. Monitoring Observance of the Law

The ICO monitors the observance of the DPA and, where necessary, implements enforcement measures against those who breach it.[105] The ICO launched a Personal Information Online Code of Practice in 2012,[106] made under section 51 of the Data Protection Act. This Code details how the Act "applies to the collection and use of personal data online [and] provides good practice advice for organisations that do business or provide services online."[107] The Code is the Information Commissioner's interpretation of "what the DPA requires when personal data is collected and used online."[108] The Code aims to fill the gap created by the requirements of the DPA, which the ICO notes "provides no guidance on the practical measures that could be taken to comply with them."[109] The Code does not apply to the collection of anonymized or statistical data.[110]

2. Enforcement

The ICO has an enforcement role and is responsible for ensuring that the provisions of the DPA are followed by any data controller, whether online or offline. The ICO has a number of both civil and criminal enforcement measures available to it. These are discussed in Part II, above, under the subheading "Sanctions."

Concerns have been raised over the duplicity of roles the ICO has, and the potential for conflicts of interest. The original rationale behind the multiple roles was the "need for the best use of resources, together with consistency of approach."[111] Commentators have noted that the enforcement function of the ICO is "arguably of central importance, with other duties, such as dissemination of information, being ancillary to this."[112]

The ICO has been behind several amendments to the DPA. For example, it had a role in the introduction of additional financial penalties under the DPA.[113]

Back to Top

## IV. Public and Scholarly Opinion

Data protection laws and subject access rights are commonly known across the UK, with the Data Protection Act consistently being the most requested piece of legislation from the UK government's online legislative database.[114] It appears that the public is becoming increasingly aware of their rights under the DPA. The ICO has noted an increase in the number of complaints over the past few years from data subjects who believe that their privacy has been breached. Since being authorized to administer financial penalties, the ICO has issued over twenty-one penalty notices totaling £2 million (approximately US$3.4 million) in fines.[115]

Back to Top

## V. Pending Reforms

The ICO is actively working with the EU on a new Data Protection Directive that aims to be "technology neutral."[116] In terms of the retention of data for the purposes of preventing crime, a new draft Communications Data Bill was recently introduced in Parliament that would update the Regulation of Investigatory Powers Act. It requires UK ISPs to retain data of a much wider range than is currently required, extending to social networking sites, webmail, and gaming site information.[117]

Back to Top

Prepared by Clare Feikert-Ahalt
Foreign Law Specialist
June 2012

---

[1] European Convention for the Protection of Human Rights and Fundamental Freedoms, *opened for signature* Nov. 4, 1950, 213 U.N.T.S. 222. The European Convention on Human Rights was incorporated into the national legislation of the United Kingdom by the Human Rights Act 1998, c. 42, sch. 1, art. 8.

[2] Data Protection Act 1998, c. 29, http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1. The UK's Data Protection Act was created to implement a European Union Directive that established a set of principles to govern the protection of data throughout the European Economic Area. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 (EC), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[3] *Data Protection Act Factsheet*, INFORMATION COMMISSIONER, http://www.aimhigher.ac.uk/practitioner/resources/Data_protection_fact_sheet.pdf (last visited June 28, 2012).

[4] "Art. 1 of the Data Protection Directive protects the privacy of an individual with respect to the processing of data; on the other hand, there is no mention of the word privacy in the Data Protection Act 1998." DIANE ROWLAND, INFORMATION TECHNOLOGY LAW 151 (2011). *See also* R v. Brown, [1996] 1 All ER 545.

[5] Data Protection Act 1998, c. 29, introductory text.

[6] Francis G.B. Aldhouse, *Data Protection, Privacy and the Media*, 4 COMM. L. 8, 11 (1999), *cited in* ROWLAND, *supra* note 4, at 152.

[7] ROWLAND, *supra* note 4, at 155.

[8] *Id*. at 167.

[9] The Information Commissioner has offered guidance, noting that data is considered to be processed when it is "collected and analysed with the intention of distinguishing one individual from another and to take a particular action in respect of an individual. This can take place even if no obvious identifiers, such as names or addresses, are held." Innovations Mail Order v. DPR, Case DA/92 31/49/1. The Information Commissioner considers that for multi-user devices, such as personal computers in shared households, if it cannot be determined whether the information collected is from an individual user or a group of users it is good practice to treat it all as personal data. Information Commissioner's Office, Personal Information Online Code of Practice 8 (July 2010), http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/personal_information_online_cop.ashx.

[10] Data Protection Act 1998, c. 29, sch. 1.

[11] *Id*., c. 29, § 1.

[12] Durant v. Financial Services Authority, [2003] EWCA Civ. 1746.

[13] *Id*.

[14] Data Protection Act 1998, c. 29, § 5.

[15] *Id*.

[16] ROSEMARY JAY & ANGUS HAMILTON, DATA PROTECTION LAW AND PRACTICE ¶ 3.46 (2d ed. 2003).

[17] Information Commissioner's Office, *supra* note 9, at 11.

[18] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:PDF.

[19] Directive 2009/136/EC on Universal Service and User's Rights Relating to Electronic Communications Networks and Services 2009 O.J. (L 377) 11, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF.

[20] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, ¶ 14, http://www.legislation.gov.uk/uksi/2003/2426/regulation/14/made, *as amended by* The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, SI 2011/1208, http://www.legislation.gov.uk/uksi/2011/1208/contents/made.

[21] *Id*. ¶ 6(1)–(2), http://www.legislation.gov.uk/uksi/2003/2426/regulation/6/made.

[22] Information Commissioner's Office, *supra* note 9, at 32.

[23] Data Protection Act 1998, c. 29.

[24] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426.

[25] Anti-terrorism, Crime and Security Act 2001, c. 24, http://www.legislation.gov.uk/ukpga/2001/24/contents.

[26] Home Office, *Retention of Communications Data Under Part 11: Anti-Terrorism, Crime and Security Act 2001, Voluntary Code of Practice*, http://www.opsi.gov.uk/si/si2003/draft/5b.pdf (last visited June 27, 2012).

[27] Anti-terrorism, Crime and Security Act 2001, c. 24, § 103, http://www.legislation.gov.uk/ukpga/2001/24/contents.

[28] *Id*. § 102.

[29] *Id*. § 104.

[30] The Data Retention (EC Directive) Regulations 2009, SI 2009/859, http://www.legislation.gov.uk/ukdsi/2009/9780111473894/contents, transposing Directive 2006/24/EC on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:PDF.

[31] Data Retention (EC Directive) Regulations 2009, *supra* note 30, sched.

[32] Information Commissioner's Office, *supra* note 9, at 12. The UK National Archives has produced guidance on how long data should be retained and when it should be deleted. *Retention and Disposal Schedules*, THE NATIONAL ARCHIVES, http://www.nationalarchives.gov.uk/information-management/projects-and-work/retention-disposal-schedules.htm (last visited May 30, 2012).

[33] Information Commissioner's Office, *supra* note 9, at 12.

[34] *Id.*

[35] The Data Retention (EC Directive) Regulations 2009, SI 2009/859.

[36] Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2009, 2009/859, http://www.legislation.gov.uk/uksi/2009/859/pdfs/uksiem_20090859_en.pdf.

[37] Data Retention (EC Directive) Regulations 2009, SI 2009/859.

[38] *Id.* § 11(1), http://www.legislation.gov.uk/uksi/2009/859/regulation/11/made.

[39] Information Commissioner's Office, *supra* note 9, at 14.

[40] *Id*. *See also Privacy Notices*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_notices.aspx (last visited June 27, 2012).

[41] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2426/2003, ¶ 6(1)–(2), http://www.legislation.gov.uk/uksi/2003/2426/regulation/6/made.

[42] Information Commissioner's Office, Privacy and Electronic Communications Regulations: Guidance on the Rules on Use of Cookies and Similar Technologies (May 2012), http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/~/media/

documents/library/Privacy_and_electronic/Practical_application/guidance_on_the_new_cookies_regulations.ashx.

[43] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2426/2003, ¶ 6(4).

[44] Data Protection Act 1998, c. 29, § 10, http://www.legislation.gov.uk/ukpga/1998/29/section/10.

[45] *iPhone Apps Exposed for Downloading Users' Data*, WHICH? NEWS (Feb. 16, 2012), http://www.which.co.uk/news/2012/02/iphone-apps-exposed-for-downloading-users-data--279395/.

[46] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, ¶ 14, http://www.legislation.gov.uk/uksi/2003/2426/regulation/14/made.

[47] *Id*.

[48] *Location Data*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/location_data.aspx (last visited June 26, 2012).

[49] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, ¶ 14(3)(a)–(c), http://www.legislation.gov.uk/uksi/2003/2426/regulation/14/made.

[50] Information Commissioner's Office, *supra* note 46.

[51] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, ¶ 14.

[52] *Child Internet Safety*, DEPARTMENT FOR EDUCATION, http://www.education.gov.uk/childrenandyoungpeople/healthandwellbeing/safeguardingchildren/a0064981/child-internet-safety (last updated Apr. 12, 2012)

[53] *Id*.

[54] *Study Reveals the UK's 'Under-age' Social Networking Generation*, LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE, http://www2.lse.ac.uk/newsAndMedia/news/archives/2011/04/UKKidsOnline.aspx (last updated Apr. 18, 2011).

[55] Press Release, School of Education, Bath Spa University, Child Protection Conference at Bath Spa University Sparks National Debate (Apr. 24, 2012), http://www.bathspa.ac.uk/about/news/default.asp?article=981.

[56] *See*, *e.g.*, *Facebook Guidance*, PEEL COMMON JUNIOR SCHOOL, http://www.peelcommon-jun.hants.sch.uk/p_Facebook_.ikml (last visited July 10, 2012).

[57] Data Protection Act 1998, c. 29, sch. 1, pt. 1, ¶ 7.

[58] *Id*. sch. 1, part II, ¶ 9.

[59] *Sending Personal Data Outside the European Economic Area (Principle 8)*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_8.aspx (last visited July 9, 2012).

[60] JISC LEGAL INFORMATION, SECURITY, MOBILE DEVICES AND DATA PROTECTION 1 (Key Points) (Feb. 2012), http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2326/Security-Mobile-Devices-and-Data-Protection.aspxhttp://www.jisclegal.ac.uk/Portals/12/Documents/Security%20Mobile%20Devices%20and%20Data%20Protection.pdf.

[61] *New EU Cookie Law (e-Privacy Directive)*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx (last visited July 9, 2012).

[62] Data Protection Act 1998, c. 29.

[63] *Id*. pt. II.

[64] *Id*.

[65] *Id*.

[66] Information Commissioner's Office, *supra* note 9, at 32.

[67] Durant v. Financial Services Authority, [2003] EWCA Civ 1746, *cited in* ROWLAND, *supra* note 4, at 175.

[68] Data Protection Act 1998, c. 29, § 7.

[69] *Id*.

[70] *Id*. § 8(2).

[71] *Id*. § 7(4).

[72] ROWLAND, *supra* note 4, at 175.

[73] Data Protection Act 1998, c. 29, § 7.

[74] Ezsias v. Glamorgan NHS Trust, [2007] EWHC 815 (QB) 53–54.

[75] *Id*.

[76] Durant v. Financial Services Authority, [2003] EWCA Civ. 1746, *cited in* ROWLAND, *supra* note 4, at 176.

[77] Data Protection Act 1998, c. 29, part IV & sch. 7.

[78] *Id*.

[79] *Id*. § 7(10).

[80] *Id*. §§ 10–12.

[81] ROWLAND, *supra* note 4, at 176.

[82] Data Protection Act 1998, c. 29, § 14.

[83] Dave Clancy, *The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/news/blog/2012/~/media/documents/library/Privacy_and_electronic/Notices/cookie_regulations_letter.ashx (last visited June 27, 2012).

[84] Criminal Justice and Immigration Act 2008, c. 4, http://www.legislation.gov.uk/ukpga/2008/4/contents.

[85] Data Protection Act 1998, c. 29, § 40(2).

[86] Information Commissioner's Office, Privacy and Electronic Communications Regulations: Guidance on the Rules on Use of Cookies and Similar Technologies, 2012, 26, http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx.

[87] *Security Breaches*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/security_breaches.aspx (last visited June 27, 2012).

[88] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, ¶ 5C, as amended, http://www.legislation.gov.uk/uksi/2003/2426/contents/made.

[89] *Enforcing the Revised Privacy and Electronic Communications Regulations (PECR)* (May 25, 2012), INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/~/media/documents/library/Privacy_and_electronic/Practical_application/enforcing_the_revised_privacy_and_electronic_communication_regulations_v1.pdf.

[90] Data Protection Act 1998, c. 29, § 55.

[91] *Id*. § 55A.

[92] Data Protection Act 1998, c. 29, § 60.

[93] *Data Protection FAQs—for Organisations*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/Global/faqs/data_protection_for_organisations.aspx#f0CFA8622-7A94-4648-840F-0BB40E91C6C5 (last visited June 26, 2012).

[94] *Id*.

[95] Data Protection Act 1998, c. 29, § 55A.

[96] *Id*. sch. 1, Part I, ¶ 8.

[97] *Id*. §§ 27–38, sch. 7, ¶ 1. There are many exemptions, including national security; crime and taxation; health, education, and social work; regulatory activities; journalism, literature, and art; research history and statistics; and corporate finance.

[98] *Id*. sch. 4.

[99] *About the ICO*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/about_us.aspx (last visited June 20, 2012).

[100] *History of the ICO*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/about_us/our_organisation/history.aspx (last visited June 20, 2012).

[101] Data Protection Act 1984, c. 35, http://www.legislation.gov.uk/ukpga/1984/35/enacted.

[102] *Key Facts*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/about_us/our_organisation/key_facts.aspx (last visited June 20, 2012).

[103] *Id*.

[104] *Id*.

[105] *Id*.

[106] Information Commissioner's Office, *supra* note 9.

[107] *Id*. at 6.

[108] *Id*. at 9.

[109] *Id*. at 8.

[110] *Id*. at 6.

[111] ROWLAND, *supra* note 4, at 182.

[112] *Id.*

[113] *Criminal Justice and Immigration Bill – ICO briefing, April 2008*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/news/current_topics/clause_76_briefing_april_2008.aspx (last visited June 30, 2012).

[114] LEGISLATION.GOV.UK, http://www.legislation.gov.uk/ (last visited June 29, 2012).

[115] *ICO Shows Its Teeth, As the Public's Concern over Illegal Marketing Calls Grows*, INFORMATION COMMISSIONER'S OFFICE (July 5, 2012), http://ico.gov.uk/news/latest_news/2012/ico-shows-its-teeth-as-the-public-concern-over-illegal-marketing-calls-grows-05072012.asp.

[116] ROWLAND, *supra* note 4, at 187.

[117] Draft Communications Data Bill, 2011–2012, Cm. 8359, http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf.

Back to Top

Last Updated: 04/02/2018