ARTICLE 29 Data Protection Working Party

10595/03/EN
WP 79

Opinion 5/2003 on the level of protection of personal data in Guernsey

Adopted on 13 June 2003

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC. The Secretariat is provided by:

Directorate E (Services, Intellectual and Industrial Property, Media and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.
Website: www.europa.eu.int/comm/privacy

OPINION OF THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA
set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

On the level of protection of personal data in Guernsey

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA,

Having regard to 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[1], and in particular Articles 29 and 30 paragraph 1 (b) thereof,

Having regard to the Rules of Procedure of the Working Party[2], and in particular Article 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION: LAW ON DATA PROTECTION IN GUERNSEY

1.1. The situation of the Channel Islands and Guernsey

The Channel Islands are a group of islands, islets and offshore rocks located in the English Channel within the Gulf of St Malo off the north-west coast of France. Although the Islands form part of the British Isles they do not form part of the United Kingdom. They are divided into the Bailiwicks of Guernsey and Jersey.
The Islands are dependencies of the Crown (being neither part of the United Kingdom nor colonies) and enjoy full independence, except for international relations and defence which are the responsibility of the United Kingdom Government. Guernsey, Alderney and Sark are each governed by separate elected Legislative Assemblies.

The position of the Bailiwick was further examined when the United Kingdom Government applied in 1971 to join the European Economic Community. The negotiated settlement granted the Channel Islands, of which the Bailiwick is an integral part, a special relationship with the European Community by virtue of Protocol 3 to the Treaty of Accession. The effect of this Protocol is that the Islands of the Bailiwick are within the Common Customs Area and the Common External Tariff of the European Community, and consequently enjoy access to Member States of physical exports of agricultural and industrial products without tariff barriers.

[1] OJ L 281, 23.11.1995, p. 31, available at: http://europa.eu.int/comm/internal_market/privacy/law_en.htm
[2] Adopted by the Working Party at its third meeting held on 11.9.1996

However, the remaining clauses of the EC Treaties do not apply to the Channel Islands and therefore for all purposes other than Customs they are effectively 'third countries'. The coming into effect of the Treaty on European Union on 1 November 1993, and the Treaty of Amsterdam on 2 October, 1997 have not altered the constitutional position as enshrined by Protocol 3 to the Treaty of Accession.

1.2. Existing data protection legal framework:

The following Conventions have been ratified on behalf of the Bailiwick:
- European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR);
- International Covenant on Civil and Political Rights;
- International Covenant on Economic, Social and Cultural Rights;
- UN Convention on the Elimination of Racial Discrimination.
- Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (convention 108).

Under the constitution of the Bailiwick, as well as its constitutional relationship with the United Kingdom, the possession of rights and freedoms is an inherent part of being a member of such a society.

Guernsey has had a data protection law since 1986. The Data Protection (Bailiwick of Guernsey) Law, 1986 was passed by the States of Guernsey on 30 July, the States of Alderney on 3 September and the Chief Pleas of Sark on 1 October, 1986.
The 1986 Law followed closely the Data Protection Act 1984 of the United Kingdom and came fully into force in November 1987. The passage of the 1986 Law enabled the United Kingdom's ratification of the Council of Europe Convention 108 in August 1987 to be extended to the Bailiwick.

On 26 July 2000 the States of Guernsey resolved to amend the data protection law with the intention of being fully compliant with Directive 95/46/EC and at the same meeting approved the establishment of an independent data protection Commissioner who in the interim would operate under the existing 1986 Law.
The Data Protection (Bailiwick of Guernsey) Law, 2001 was approved by the States of Guernsey on 28 November 2001, by the States of Alderney on 23 January and by the Chief Pleas of Sark on 16 January 2002. The Law follows closely the UK Data Protection Act 1998.
The Law obtained Royal Assent on 26 March and came fully into force on 1 August 2002, when some 16 Statutory Instruments were also made. These, again, mirrored for the most part those in force in the United Kingdom, but were modified to take account of differences in the legislative environment in the Bailiwick.
The passage of the Law has enabled the Bailiwick authorities to confirm that the UK may extend its ratification of the Additional Protocol to the Convention regarding supervisory authorities and transborder data flows to the Bailiwick, although this has yet to be done.

The general philosophy behind the new Law has been to draft data protection legislation to follow the UK legislation as closely as possible. This approach has been justified by the following reasons:
a) it gives greater certainty that the requirements of the Directive will have been transposed adequately;

b) it simplifies the compliance procedures for data controllers established in the Bailiwick, since many of them are associated with organisations based in the UK;
c) it enables the Commissioner to exploit access to expertise, literature and advice from the Office of the UK Information Commissioner
d) it allows the re-use of notification software (and procedures) originally developed for the UK.

2. ASSESSMENT OF THE DATA PROTECTION LAW OF GUERNSEY AS PROVIDING ADEQUATE PROTECTION OF PERSONAL DATA

The Working Party points out that its assessment on the adequacy of the Law on data protection in Guernsey focuses on the Data Protection (Bailiwick of Guernsey) Law, 2001.

The provisions of this Law have been compared with the main provisions of the Directive, taking into account the Working Party's opinion on "Transfers of personal data to third countries; Applying Articles 25 and 26 of the EU data protection Directive[3]". This opinion lists a number of principles which constitute *a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate*. In order to facilitate the reading of the text, the wording of long articles of the Law has been included as annex. The result of this analysis is as follows:

2.1. Content Principles

Basic principles

- **the purpose limitation principle -** data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.

The Working Party is satisfied that the Law of Guernsey complies with this principle. Schedule 1, part 1 and in particular the second principle sets out that "*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*". Further, the fifth principle of the same schedule adds: *"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes"*.

- **the data quality and proportionality principle -** data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

The Working Party understands that this principle is complied with by the Law of Guernsey. Schedule 1, part 1, and in particular the third principle, provides that *"Personal data shall be adequate, relevant and not excessive in relation to the*

[3] WP 12 – Adopted by the Working Party on 24 July 1998, available at: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

purpose or purposes for which they are processed". Further, the fourth principle of the same schedule stipulates that "*Personal data shall be accurate and, where necessary, kept up to date."*.

- **the transparency principle -** individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the directive**.**

The Working Party notes that this principle is complied with by the Law of Guernsey, in particular, by its Article 7 (see annex, number 1). This principle is further developed in schedule 1, part 2, numbers 2 and 3 (annex, number 2).

- **the security principle** - technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

The Working Party understands that the Law of Guernsey complies with this principle. Schedule 1, part 1, seventh principle, provides as follows:
"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."

This principle is further explained in the second part of the same schedule and in particular in numbers 9 to 12 (annex, number 3).

- **the rights of access, rectification and opposition -** the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.

As for the right of access, the Working Party is satisfied that this principle is complied with by this Law, in particular by its Article 7 (annex, number 4). This principle is further developed in its Article 8.

As for the right of rectification, the Working Party understands that this principle is complied with by the Law of Guernsey. In particular, Article 14 of the Law deals with the rights of rectification, blocking, erasure and destruction (annex, number 5).

The right of opposition is dealt with in Article 10. Article 10 establishes the right to prevent processing likely to cause damage or distress (annex, number 6).

The exceptions to the right of access are contained in the secondary legislation[4], allowing for well-defined restrictions in a number of specific cases:

[4] In particular the Miscellaneous Subject Access Exemptions Order 2002, the Subject Access Modification (Education) Order 2002, the Subject Access Modification (Health) Order 2002 and the Subject Access Modification (Social Work) Order 2002.

- personal data the disclosure of which is prohibited or restricted by certain enactments and subordinate instruments in the interests of safeguarding the interests of the data subject himself or the rights and freedoms of some other individual (article 1).The personal data exempted concern adoption records and reports in Guernsey and Alderney;
- certain data (education records) where the exercise of those rights would be likely to cause serious harm to the physical or mental health or condition of the data subject or another person, or, in some circumstances, would disclose information as to whether the data subject is or has been the subject of or may be at risk of child abuse which disclosure would not be in the best interests of that data subject;
- when the supply to the data subject of particulars of the information constituting the data would be likely to cause serious harm to his or any other person's physical or mental health or condition. Before deciding whether this exemption applies (and, accordingly, whether to grant or withhold subject access) a data controller who is not a health professional is obliged by articles 3(2) and 4(1) to consult the health professional responsible for the clinical care of the data subject or, if there is more than one, the most suitable available health professional or, if there is none available or the data controller is the States' Board of Health, the States' Social Security Authority, a probation officer or other person in the course of any proceedings relating to families or children, a health professional who has the necessary experience and qualifications to advise on the matters to which the information which is requested relates (definition in article 7).
- in certain circumstances where a third party is making the request for access on behalf of the data subject and the data subject does not wish that information to be disclosed to that third party;
- certain data where the exercise of those rights would be likely to prejudice the carrying out of social work by causing serious harm to the physical or mental health or condition of the data subject or another person.

The Working Party considers that these exceptions are in line with the provisions of Article 13 of the Directive.

- **restrictions on onward transfers -** further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive.

The Working Party understands that this principle is complied with by the Law of Guernsey. In particular, schedule 1, part 1, eight principle reads as follows: "*Personal data shall not be transferred to a country or territory outside the Bailiwick 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"*. This principle is further explained in schedule 1, part 2, numbers 13 to 15 (annex, number 7).

The exceptions to this principle are contained in Schedule 4 (annex, number 8). The Working Party notes with satisfaction that these exceptions are perfectly in line with article 26 of the Directive.

Additional principles to be applied to specific types of processing are:

- **sensitive data** - where 'sensitive' categories of data are involved (those listed in Article 8 of the directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

The Working Party understands that this principle is complied with the Law of Guernsey. In particular, Article 2 of the Law defines "sensitive data" as (annex, number 9).

Schedule 1, part 1, principle 1, letter b adds that sensitive data shall not be processed unless one of the conditions of Schedule 3 are met (annex, number 10).

- **direct marketing** - where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.

The Working Party notes that this principle is complied with by Article 11, that regulates the right to prevent processing for purposes of direct marketing (annex, number 11).

- **automated individual decision** - where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

The Working Party understands that this principle is complied with by the Law in Guernsey. In particular, by its Article 7.1, letter d (annex, number 12) and its Article 12 that elaborates on the rights in relation to automated decision taking (annex, number 13).

2.2. Procedural/ Enforcement mechanisms

The Working Party's opinion on "Transfers of personal data to third countries; Applying Articles 25 and 26 of the EU data protection Directive"[5] indicates that the assessment of the adequacy of a third country's legal system should identify the underlying objectives of a data protection procedural system, and on this basis judge the variety of different judicial and non-judicial procedural mechanisms used in third countries.

With that regard, the objectives of a data protection system are essentially threefold:

– to deliver a good level of compliance with the rules;
– to provide support and help to individual data subjects in the exercise of their rights;
– to provide appropriate redress to the injured party where rules are not complied with.

- **to deliver a good level of compliance with the rules** - A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important

[5] WP 12 – Adopted by the Working Party on 24 July 1998, available at: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

The Working Party understands that the Law of Guernsey has put in place a number of elements to serve this objective. In particular:

(a) Data Protection Commissioner

The Law of Guernsey provides in its Article 6 for the office originally established by section 33A of the Data Protection (Bailiwick of Guernsey) Law, 1986 and known as the Data Protection Commissioner to continue to exist for the purposes of this Law.

The Commissioner is fully independent, as stated in Article 6.4 of the Law: *The Commissioner is not a servant or agent of the States, but is a holder of public office and is under a duty to discharge the functions of that office with complete fairness, impartiality and independence.*

The Commissioner has a comprehensive list of duties, specified in Article 51 of the Law (annex, number 14). The Commissioner is endowed with a number of powers, such as the powers of entry and inspection[6] and the power to issue information and enforcement notices[7]. A person who fails to comply with an enforcement notice, an information notice or a special information notice shall be guilty of an offence[8].

(b) The existence of adequate enforcement means and sanctions

The Law provides for a number of offences:-
a) Failure to notify or to notify changes to an entry.
b) Unauthorised disclosure of data, or selling of data or obtaining of data.
c) Failure to comply with a notice.
d) obstruction of a person in the execution of a warrant.

The Commissioner may serve an enforcement notice where he has assessed that a controller is not complying with the principles or an information notice where he needs more information to complete an assessment.

Complaints by data subjects to the Commissioner concerning notification or disclosure offences would be dealt with as potential criminal prosecutions by the Law Officers.
Complaints involving non-compliance with principles are dealt with as a request for assessment. Only if a data controller fails to comply with an enforcement or information notice issued during the assessment process would a prosecution be contemplated.

Article 60 of the Law deals with prosecution and offences (annex, number 15). As stated before, a person who fails to comply with an enforcement notice, an information notice or a special information notice shall be guilty of an offence. The

[6] See Article 50 of the Law as well as Schedule 8.
[7] See Articles 40 and 43 of the Law.
[8] See Article 47 of the Law.

same applies for any person failing to comply with the duty imposed by notification regulations[9]

In the view of these considerations, the Working Party understands that Law of Guernsey contains the elements necessary to deliver a good level of compliance with the rules.

- **to provide support and help to individual data subjects in the exercise of their rights -** The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

The Working Party notes that the Law of Guernsey has put in place a number of elements to serve this objective. In particular, citizens can ask the Commissioner to make an assessment. This is regulated in Article 22 of the Law (annex, number 16).
The procedure for assessment is described in detail on the Commissioner´s website and it involves no cost for the individuals. It is also important to note that a scheme of legal aid exists in Guernsey to allow individuals to go to Court for civil claims.

In the view of these considerations, the Working Party understands that the Law of Guernsey contains the elements necessary to provide support and help to individual data subjects in the exercise of their rights.

- **to provide appropriate redress to the injured party where rules are not complied with** - This is a key element, which must involve a system of independent adjudication, or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

The Law of Guernsey provides for a compensation scheme in Article 13 (annex, number 17).

In the view of these considerations, the Working Party understands that that Law of Guernsey contains the elements necessary to provide appropriate redress to the injured party where rules are not complied with.

[9] See Article 21 of the Law.

3. RESULTS OF THE ASSESSMENT

In conclusion, on the basis of the above mentioned findings, the Working Party is satisfied that Guernsey ensures an adequate level of protection within the meaning of Article 25(6) of 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.

Done at Brussels, on 13 June 2003

For the Working Party
The Chairman
Stefano RODOTA

Annex: Relevant provisions of the Guernsey Data Protection Law

(1)*"(1)Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled-*

(a)to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller;

(b)if that is the case, to be given by the data controller a description of-

(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;

(c)to have communicated to him in an intelligible form-

(i)the information constituting any personal data of which that individual is the data subject; and

(ii)any information available to the data controller as to the source of those data; and

(d)where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking."

(2) *"2.(1)Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless-*

(a)in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3); and

(b)in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).

*(2)In sub-paragraph (1)(b) "**the relevant time**" means-*

(a)the time when the data controller first processes the data; or

(b)in a case where at that time disclosure to a third party within a reasonable period is envisaged-

(i)if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed;

(ii)if within that period the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware; or

(iii)in any other case, the end of that period.

(3)The information referred to in sub-paragraph (1) is as follows, namely-

(a)the identity of the data controller;

(b)if he has nominated a representative for the purposes of this Law, the identity of that representative;

(c)the purpose or purposes for which the data are intended to be processed; and

(d)any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in

respect of the data subject to be fair.
3.(1)Paragraph 2(1)(b) does not apply where either of the primary conditions in sub-paragraph (2), together with such further conditions as may be prescribed by the Committee by Order, are met.
(2)The primary conditions referred to in sub-paragraph (1) are-
(a)that the provision of that information would involve a disproportionate effort; or
(b)that the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract".

(3) *"9.Having regard to the state of technological development and the cost of implementing any measures, the measures 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.
10.The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.
11.Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle-
(a)choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
(b)take reasonable steps to ensure compliance with those measures.
12.Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless-
(a)the processing is carried out under a contract-
(i)which is made or evidenced in writing; and
(ii)under which the data processor is to act only on instructions from the data controller; and
(b)the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle".

(4) *(1)Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled-*
(a)to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller;
(b)if that is the case, to be given by the data controller a description of-
(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;
(c)to have communicated to him in an intelligible form-
(i)the information constituting any personal data of which that individual is the data subject; and
(ii)any information available to the data controller as to the source of those data; and
(d)where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for

example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking.

(2)A data controller is not obliged to supply any information under subsection (1) unless he has received-

(a) a request in writing; and

(b)except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require.

(3)Where a data controller-

(a)reasonably requires further information in order to satisfy himself as to the identity of the person making a request under this section and to locate the information which that person seeks; and

(b)has informed him of that requirement,

the data controller is not obliged to comply with the request unless he is supplied with that information.

(4)Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless-

(a)the other individual has consented to the disclosure of the information to the person making the request; or

(b)it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

(5)In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing a data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.

(6)In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to-

(a)any duty of confidentiality owed to the other individual;

(b)any steps taken by the data controller with a view to seeking the consent of the other individual;

(c)whether the other individual is capable of giving consent; and

(d)any express refusal of consent by the other individual.

(7)An individual making a request under this section may, in such cases as may be prescribed, specify that his request is limited to personal data of any prescribed description.

(8)Subject to subsection (4), a data controller shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.

(9)If a court is satisfied on the application of any person who has made a request under the foregoing provisions of this section that the data controller in question has failed to comply with the request in contravention of those provisions, the court may order him to comply with the request.

(10)For the purpose of determining any question whether an applicant under subsection (9) is entitled to the information which he seeks (including any question

whether any relevant data are exempt from that section by virtue of Part IV) the court may require the information constituting any data processed by or on behalf of the data controller and any information as to the logic involved in any decision-taking as mentioned in subsection (1)(d) to be made available for its own inspection but shall not, pending the determination of that question in the applicant's favour, require the information sought by the applicant to be disclosed to him or his representatives whether by discovery or otherwise.
(11)In this section-
*"**prescribed**" means prescribed by the Committee by regulations;*
*"**the prescribed maximum**" means such amount as may be prescribed;*
*"**the prescribed period**" means sixty days or such other period as may be prescribed; and*
*"**the relevant day**", in relation to a request under this section, means the day on which the data controller receives the request or, if later, the first day on which the data controller has both the required fee and the information referred to in subsection (3).*
(12)Different amounts or periods may be prescribed under this section in relation to different cases."

(5) " *14.(1)If a court is satisfied on the application of a data subject that personal data of which the applicant is the subject are inaccurate, the court may order the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which he is the data controller and which contain an expression of opinion which appears to the court to be based on the inaccurate data.*
(2)Subsection (1) applies whether or not the data accurately record information received or obtained by the data controller from the data subject or a third party but where the data accurately record such information, then-
(a)if the requirements mentioned in paragraph 7 of Part II of Schedule 1 have been complied with, the court may, instead of making an order under subsection (1), make an order requiring the data to be supplemented by such statement of the true facts relating to the matters dealt with by the data as the court may approve; and
(b)if all or any of those requirements have not been complied with, the court may, instead of making an order under that subsection, make such order as it thinks fit for securing compliance with those requirements with or without a further order requiring the data to be supplemented by such a statement as is mentioned in paragraph (a).
(3)Where the court-
(a)makes an order under subsection (1); or
(b)is satisfied on the application of a data subject that personal data of which he was the data subject and which have been rectified, blocked, erased or destroyed were inaccurate;
it may, where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.
(4)If a court is satisfied on the application of a data subject-
(a)that he has suffered damage by reason of any contravention by a data controller of any of the requirements of this Law in respect of any personal data, in circumstances entitling him to compensation under section 13; and
(b)that there is a substantial risk of further contravention in respect of those data in such circumstances;

the court may order the rectification, blocking, erasure or destruction of any of those data.
(5)Where the court makes an order under subsection (4) it may, where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.
(6)In determining whether it is reasonably practicable to require such notification as is mentioned in subsection (3) or (5) the court shall have regard, in particular, to the number of persons who would have to be notified".

(6) *"(1)Subject to subsection (2), an individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject, on the ground that, for specified reasons-*
(a)the processing of those data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another; and
(b)that damage or distress is or would be unwarranted.
(2)Subsection (1) does not apply-
(a)in a case where any of the conditions in paragraphs 1 to 4 of Schedule 2 is met; or
(b)in such other cases as may be prescribed by the Committee by Order.
*(3)The data controller must within twenty-one days of receiving a notice under subsection (1) (**"the data subject notice"**) give the individual who gave it a written notice-*
(a)stating that he has complied or intends to comply with the data subject notice; or
(b)stating his reasons for regarding the data subject notice as to any extent unjustified and the extent (if any) to which he has complied or intends to comply with it.
(4)If a court is satisfied, on the application of any person who has given a notice under subsection (1) which appears to the court to be justified (or to be justified to any extent), that the data controller in question has failed to comply with the notice, the court may order him to take such steps for complying with the notice (or for complying with it to that extent) as the court thinks fit.
(5)The failure by a data subject to exercise the right conferred by subsection (1) or section 11(1) does not affect any other right conferred on him by this Part".

(7) *"13.An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to-*
(a)the nature of the personal data;
(b)the country or territory of origin of the information contained in the data;
(c)the country or territory of final destination of that information;
(d)the purposes for which and period during which the data are intended to be processed;
(e)the law in force in the country or territory in question;
(f)the international obligations of that country or territory;
(g)any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases); and
(h)any security measures taken in respect of the data in that country or territory.
14.The eighth principle does not apply to a transfer falling within any paragraph of Schedule 4, except in such circumstances and to such extent as the Committee may by Order provide.

15.(1)Where-
(a)in any proceedings under this Law any question arises as to whether the requirement of the eighth principle as to an adequate level of protection is met in relation to the transfer of any personal data to a country or territory outside the Bailiwick; and
(b)a Community finding has been made in relation to transfers of the kind in question; that question is to be determined in accordance with that finding.
*(2)In sub-paragraph (1) "**Community finding**" means a finding of the European Commission, under the procedure provided for in Article 31(2) of the Data Protection Directive, that a country or territory outside the European Economic Area does, or does not, ensure an adequate level of protection within the meaning of Article 25(2) of the Directive".*

(8) *"1.The data subject has given his consent to the transfer.*
2.The transfer is necessary-
(a)for the performance of a contract between the data subject and the data controller; or
(b)for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller.
3.The transfer is necessary-
(a)for the conclusion of a contract between the data controller and a person other than the data subject which-
(i)is entered into at the request of the data subject; or
(ii)is in the interests of the data subject; or
(b)for the performance of such a contract.
4.(1)The transfer is necessary for reasons of substantial public interest.
(2)The Committee may by Order specify-
(a)circumstances in which a transfer is to be taken for the purposes of sub-paragraph (1) to be necessary for reasons of substantial public interest; and
(b)circumstances in which a transfer which is not required by or under an enactment is not to be taken for the purpose of sub-paragraph (1) to be necessary for reasons of substantial public interest.
5.The transfer-
(a)is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
(b)is necessary for the purpose of obtaining legal advice; or
(c)necessary for the purposes of establishing, exercising or defending legal rights.
6.The transfer is necessary in order to protect the vital interests of the data subject.
7.The transfer is of part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer.
8.The transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects.
9. The transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects".

(9) *"**2.** In this Law "**sensitive personal data**" means personal data consisting of information as to-*
(a)the racial or ethnic origin of the data subject;

(b)his political opinions;
(c)his religious beliefs or other beliefs of a similar nature;
(d)whether he is a member of a labour organisation, such as a trade union;
(e)his physical or mental health or condition;
(f)his sexual life;
(g)the commission or alleged commission by him of any offence; or
(h)any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings".

(10) *"1.The data subject has given his explicit consent to the processing of the personal data.*
2.(1)The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
(2)The Committee may by Order-
(a)exclude the application of sub-paragraph (1) in such cases as may be specified; or
(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
3.The processing is necessary-
(a)in order to protect the vital interests of the data subject or another person, in a case where-
(i)consent cannot be given by or on behalf of the data subject; or
(ii)the data controller cannot reasonably be expected to obtain the consent of the data subject; or
(b)in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4.The processing-
(a)is carried out in the course of its legitimate activities by any body or association which-
(i)is not established or conducted for profit; and
(ii)exists for political, philosophical, religious or trade-union purposes;
(b)is carried out with appropriate safeguards for the rights and freedoms of data subjects;
(c)relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and
(d)does not involve disclosure of the personal data to a third party without the consent of the data subject.
5.The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
6.The processing-
(a)is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
(b)is necessary for the purpose of obtaining legal advice; or
(c)is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
7.(1)The processing is necessary-
(a)for the administration of justice;
(b)for the exercise of any functions conferred on any person by or under an

enactment; or
(c)for the exercise of any functions of the Crown, a Law Officer of the Crown or a committee of the States.
(2)The Committee may by Order-
(a)exclude the application of sub-paragraph (1) in such cases as may be specified; or
(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
8.(1)The processing is necessary for medical purposes and is undertaken by-
(a)a health professional; or
(b)a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
*(2)In this paragraph "**medical purposes**" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.*
9.(1)The processing-
(a)is of sensitive personal data consisting of information as to racial or ethnic origin;
(b)is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and
(c)is carried out with appropriate safeguards for the rights and freedoms of data subjects.
(2)The Committee may by Order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.
10.The personal data are processed in circumstances specified in an Order made by the Committee for the purposes of this paragraph."

(11) "*(1)An individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which he is the data subject.*
(2)If a court is satisfied, on the application of any person who has given a notice under subsection (1), that the data controller has failed to comply with the notice, the court may order him to take such steps for complying with the notice as the court thinks fit.
*(3)In this section "**direct marketing**" means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals".*

(12) *"(1)Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled-*
(d)where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking."

(13) *"(1)An individual is entitled at any time, by notice in writing to any data controller, to require the data controller to ensure that no decision taken by or on behalf of the data controller which significantly affects that individual is based solely on the processing by automatic means of personal data in respect of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct.*
(2)Where, in a case where no notice under subsection (1) has effect, a decision which significantly affects an individual is based solely on such processing as is mentioned in subsection (1)-
(a)the data controller must as soon as reasonably practicable notify the individual that the decision was taken on that basis; and
(b)the individual is entitled, within twenty-one days of receiving that notification from the data controller, by notice in writing to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis.
*(3)The data controller must, within twenty-one days of receiving a notice under subsection (2)(b) ("**the data subject notice**") give the individual a written notice specifying the steps that he intends to take to comply with the data subject notice.*
(4)A notice under subsection (1) does not have effect in relation to an exempt decision; and nothing in subsection (2) applies to an exempt decision.
*(5)In subsection (4) "**exempt decision**" means any decision-*
(a)in respect of which the condition in subsection (6) and the condition in subsection (7) are met; or
(b)which is made in such other circumstances as may be prescribed by the Committee by Order.
(6)The condition in this subsection is that the decision-
(a)is taken in the course of steps taken-
(i)for the purpose of considering whether to enter into a contract with the data subject;
(ii)with a view to entering into such a contract; or
(iii)in the course of performing such a contract; or
(b)is authorised or required by or under any enactment.
(7)The condition in this subsection is that either-
(a)the effect of the decision is to grant a request of the data subject; or
(b)steps have been taken to safeguard the legitimate interests of the data subject (for example, by allowing him to make representations).
*(8)If a court is satisfied on the application of a data subject that a person taking a decision in respect of him ("**the responsible person**") has failed to comply with subsection (1) or (2)(b), the court may order the responsible person to reconsider the decision, or to take a new decision which is not based solely on such processing as is mentioned in subsection (1).*
(9)An Order under subsection (8) shall not affect the rights of any person other than the data subject and the responsible person".

(14) *"(1)It shall be the duty of the Commissioner to promote the following of good practice by data controllers and, in particular, so to perform his functions under this Law as to promote the observance of the requirements of this Law by data controllers.*
(2)The Commissioner shall arrange for the dissemination in such form and manner as he considers appropriate of such information as it may appear to him expedient to give to the public about the operation of this Law, about good practice, and about

other matters within the scope of his functions under this Law, and may give advice to any person as to any of those matters.
(3) Where-
(a)the Committee so directs by Order; or
(b)the Commissioner considers it appropriate to do so;
the Commissioner shall, after such consultation with trade associations, data subjects or persons representing data subjects as appears to him to be appropriate, prepare and disseminate to such persons as he considers appropriate codes of practice for guidance as to good practice.
(4)The Commissioner shall also-
(a)where he considers it appropriate to do so, encourage trade associations to prepare, and to disseminate to their members, such codes of practice; and
(b)where any trade association submits a code of practice to him for his consideration, consider the code and, after such consultation with data subjects or persons representing data subjects as appears to him to be appropriate, notify the trade association whether in his opinion the code promotes the following of good practice.
(5)An Order under subsection (3) shall describe the personal data or processing to which the code of practice is to relate, and may also describe the persons or classes of persons to whom it is to relate.
(6)The Commissioner shall arrange for the dissemination in such form and manner as he considers appropriate of-
(a)any Community finding as defined by paragraph 15(2) of Part II of Schedule 1;
(b)any decision of the European Commission, under the procedure provided for in Article 31(2) of the Data Protection Directive, which is made for the purposes of Article 26(3) or (4) of the Directive; and
(c)such other information as it may appear to him to be expedient to give to data controllers in relation to any personal data about the protection of the rights and freedoms of data subjects in relation to the processing of personal data in countries and territories outside the Bailiwick.
(7)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.
(8)The Commissioner may charge such sums as he may with the consent of the Committee determine for any services provided by the Commissioner by virtue of this Part.
(9)In this section-
*"**good practice**" means such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, and includes (but is not limited to) compliance with the requirements of this Law;*
*"**trade association**" includes any body representing data controllers".*

(15) *"1) A person guilty of an offence under any provision of this Law other than paragraph 11 of Schedule 8 is liable-*
(a) on summary conviction, to a fine not exceeding level 5 on the uniform scale; or
(b) on conviction on indictment, to a fine.
(2) A person guilty of an offence under paragraph 11 of Schedule 8 is liable on summary conviction to a fine not exceeding level 5 on the uniform scale.
(3) Subject to subsection (4), the court by or before which a person is convicted of-

(a) an offence under section 21(1), 22(6), 55 or 56;
(b) an offence under section 21(2) relating to processing which is assessable processing for the purposes of section 22; or
(c) an offence under section 47(1) relating to an enforcement notice;
may order any document or other material used in connection with the processing of personal data and appearing to the court to be connected with the commission of the offence to be forfeited, destroyed or erased.
(4)The court shall not make an order under subsection (3) in relation to any material where a person (other than the offender) claiming to be the owner of or otherwise interested in the material applies to be heard by the court, unless an opportunity is given to him to show cause why the order should not be made".

(16) *"(1)In this section "**assessable processing**" means processing which is of a description specified in an Order made by the Committee as appearing to it to be particularly likely-*
(a)to cause substantial damage or substantial distress to data subjects; or
(b)otherwise significantly to prejudice the rights and freedoms of data subjects.
(2)On receiving notification from any data controller under section 18 or under notification regulations made by virtue of section 20 the Commissioner shall consider-
(a)whether any of the processing to which the notification relates is assessable processing; and
(b)if so, whether the assessable processing is likely to comply with the provisions of this Law.
(3)Subject to subsection (4), the Commissioner shall, within the period of twenty-eight days beginning with the day on which he receives a notification which relates to assessable processing, give a notice to the data controller stating the extent to which the Commissioner is of the opinion that the processing is likely or unlikely to comply with the provisions of this Law.
(4)Before the end of the period referred to in subsection (3) the Commissioner may, by reason of special circumstances, extend that period on one occasion only by notice to the data controller by such further period not exceeding fourteen days as the Commissioner may specify in the notice.
(5)No assessable processing in respect of which a notification has been given to the Commissioner as mentioned in subsection (2) shall be carried on unless either-
(a)the period of twenty-eight days beginning with the day on which the notification is received by the Commissioner (or, in a case falling within subsection (4), that period as extended under that subsection) has elapsed; or
(b)before the end of that period (or that period as so extended) the data controller has received a notice from the Commissioner under subsection (3) in respect of the processing.
(6)Where subsection (5) is contravened, the data controller shall be guilty of an offence.
(7)The Committee may by Order amend subsections (3), (4) and (5) by substituting for the number of days for the time being specified there a different number specified in the order".

(17) *"(1)An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Law is entitled to compensation from the data controller for that damage.*
(2)An individual who suffers distress by reason of any contravention by a data

controller of any of the requirements of this Law is entitled to compensation from the data controller for that distress if-

(a)the individual also suffers damage by reason of the contravention; or

(b)the contravention relates to the processing of personal data for the special purposes.

(3)In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned".