AN BILLE UM CHOSAINT SONRAÍ, 1987
DATA PROTECTION BILL, 1987

Mar a ritheadh ag dhá Theach an Oireachtais
As passed by both Houses of the Oireachtas

EXPLANATORY MEMORANDUM

Object of Bill

1. The Bill is designed to protect the privacy of individuals with regard to automated personal data and to give effect to the Council of Europe Data Protection Convention. The text of the Convention is given in the *First Schedule* to the Bill.

Main features

2. These are:

(1) The Bill entitles individuals to establish the existence of automated personal data kept in relation to them; to have access to the data (with some exceptions); and to have inaccurate data rectified or erased (*sections 3* to *6*).

(2) It imposes various obligations on persons who keep automated personal data, e.g., the data must be accurate, be kept for lawful purposes, not be disclosed in any manner incompatible with those purposes and be protected by adequate security measures (*section 2*). In general, persons keeping such data will owe a duty of care to the data subjects concerned to the extent that the law of torts does not already so provide (*section 7*).

(3) It provides for the appointment by the Government of a Data Protection Commissioner with power to investigate complaints, to supervise the operation of the legislation and, where necessary, to require compliance with its provisions (*sections 9* to *12*).

(4) The Commissioner will encourage the preparation of codes of practice by bodies representing categories of data controllers. These codes, if approved of by each House of the Oireachtas, will have the force of law (*section* 13).

(5) Certain categories of persons and bodies who keep personal data will be required to register with the Commissioner, e.g. the public sector, financial institutions, insurance companies, direct marketing, credit reference, debt collecting and data processing agencies and those who keep particularly sensitive data (political opinions, health, criminal convictions etc.) (*section 16* and *Third Schedule*).

(6) The Commissioner will be obliged to accept applications for registration unless he has not been given sufficient information or he

considers that the applicants are likely to contravene the provisions of the Act. However, in the case of the particularly sensitive data referred to, he will be obliged to refuse registration, unless he considers that appropriate safeguards for protecting privacy are being, and will continue to be, provided by the applicants (*section 17*).

(7) In general, a failure or refusal by a person or body who keeps personal data to comply with the obligations imposed by the Bill, including the obligation to give access to data and to rectify or erase inaccurate data, will not constitute an offence; but the Commissioner may require steps to be taken to comply with the obligation in question and non-compliance with a requirement, without reasonable excuse, will be an offence (*section 10 (8)*). It will also be an offence not to register when required by the Act to do so or, being registered, knowingly to deal with personal data otherwise than in accordance with the intentions stated when applying for registration (*section 19 (6)*).

(8) Decisions of the Commissioner will be subject to appeal to the Circuit Court *(section 26)*.

(9) *Section 35 (2)*, which authorises the Minister for Justice to bring different provisions of the Bill into operation on different dates, will be utilised so as to bring into operation the provisions necessary to enable the Convention to be ratified as soon as possible consistent with the need to allow persons and bodies who keep personal data reasonable time to adjust to the requirements of the legislation and, where necessary, to become registered.

(10) The Bill does not apply to personal data kept for state security purposes or required by law to be made available to the public by the data controller concerned or kept by an individual only for recreational etc. purposes; to personal data kept on manual files; or to non-personal data, e.g. data concerning companies or partnerships.

Provisions of Bill

Preliminary

3. ***Section 1*** contains the definitions and also provides for the application of the Bill in relation to civil servants and gardaí and for the exclusion of certain personal data. "Data" are defined as information in a form in which it can be "processed", i.e. in a form in which logical or arithmetical operations can be performed automatically on it. "Personal data" are data relating to a living individual who can be identified from the data or from the data and other information in the possession of a data controller. "Data controllers" are persons who, either alone or with others, control the contents and use of automated personal data. "Data processors" are those who process personal data for others or allow processing equipment in their possession to be used by others, but the definition does not include a data controller's staff. "Data subject" is an individual about whom personal data are kept (*subsection (1)*). *Subsection (2)* defines inaccurate data as data that are inaccurate or misleading as to any matter of fact, as distinct from opinion.

4. *Section 1 (3)* provides that an "appropriate authority", as defined in the Civil Service Regulation Acts, 1956 and 1958 — e.g. a Government Minister — may designate a civil servant in his or her department to be a data controller or data processor for the purposes of the Act as regards the personal data within that civil servant's area of responsibility. In departments with a number of different functions, it may be necessary for the Minister to designate a civil servant in

each of the different areas. (The intention is that each civil servant so designated would be the subject of a separate entry in the register kept by the Data Commissioner under *section 16 (2)*.) The Minister for Defence may designate a commissioned officer for these purposes in relation to Defence Forces data. While a designation is in force, the Act will not apply to the designating authority.

5. *Section 1 (3) (c)* is a technical provision deeming civil servants and members of the Defence Forces to be employees of the "appropriate authority" or the Minister for Defence as the case may be. Members of the Garda Síochána are also deemed to be employees of the Garda Commissioner. Without such a provision, the obligations imposed by the Bill on employees of data controllers and data processors would not apply to civil servants, members of the Defence Forces or gardaí, since they are not in an employee/employer relationship with Ministers, superior ranks or the Garda Commissioner respectively. Where a civil servant or an officer has been designated, civil servants in the relevant Department or members of the Defence Forces are deemed to be employees of that civil servant or officer.

6. The Bill does not apply to personal data that, in the opinion of the Minister for Justice or the Minister for Defence, are or at any time were held for the purpose of safeguarding the security of the State; data that are required by law to be made available to the public by the data controller concerned; or data that are kept by an individual in connection with the management of his or her personal, family or household affairs or only for recreational purposes (*subsection (4)*).

Protection of Privacy of Individuals with regard to Personal Data

7. ***Section 2*** imposes on data controllers obligations in relation to the collection, accuracy, adequacy, relevance, storage and security of personal data kept by them and prohibits the use or disclosure of the data in any manner incompatible with the specified and lawful purposes for which they are kept. The obligation relating to the security of data is the only one imposed on data processors. (A failure or refusal by a data controller to comply with these provisions or with requests under *sections 3, 4* and *6* for information about, access to, or rectification or erasure of, personal data will not constitute an offence but the Commissioner, either on his own initiative or after investigating a complaint from the data subject, may issue an enforcement notice under *section 10* requiring the data controller to comply with these provisions or requests. Failure or refusal, without reasonable excuse, to comply with an enforcement notice will be an offence. However, if a data controller is within the categories required to register (see *section 16 (1)* and the *Third Schedule*), he will commit an offence if *inter alia* he knowingly keeps or uses personal data for a purpose other than the purpose or purposes described in the relevant entry in the register or if he discloses data to a person not described in the entry (other than a person to whom *section 8* allows a disclosure to be made).)

8. *Subsections (3)* to *(5)* of *section 2* modify these obligations in certain cases. The obligation to obtain and process data fairly will not apply to data kept for crime prevention, tax collection etc. if, in any particular case, compliance with the obligation would be likely to prejudice any of these matters. For example, the prevention of crime may require information to be obtained by observation of a data subject without his knowledge and that might not, in other circumstances, be regarded as fair. Back-up data, which are necessarily inaccurate between updatings, are exempted from the obligation to be accurate and up-to-date. *Subsection (5)* contains an exemption for

personal data obtained for a particular purpose and subsequently used for historical, statistical or research purposes. These data are deemed not to have been obtained in breach of the "fair collection" obligation and may be kept for an indefinite period, so long as they are not used in any way that would cause damage or distress to any data subject.

9. *Section 2 (6)* authorises the Minister for Justice to make regulations amending *subsection (1)* to provide additional safeguards in relation to personal data as to racial origin, political opinions, religious or other beliefs, physical or mental health, sexual life or criminal convictions.

10. *Section 2 (7)* entitles a data subject to have his or her name removed from a direct marketing or direct mailing list.

11. ***Section 3*** entitles an individual to establish the existence of personal data and to be given a description of the data and the purposes for which they are held (article 8a. of the Convention).

12. ***Section 4*** is complementary to *section 3* and gives a right to the individual concerned to be supplied, within 40 days, with a copy of any personal data about him on making a request in writing to the data controller and on payment of any fee required (article 8b. of the Convention). The fee must not exceed whichever is the lesser of the following amounts: that prescribed by the Minister with the consent of the Minister for Finance or an amount that in the opinion of the Commissioner is reasonable having regard to the estimated cost to the data controller of complying with the request for access. A fee is refundable if the request is not complied with or the data are materially modified (*subsection (1)*). Where a data controller is required to register under the Bill (*section 16* and the *Third Schedule*) and separate entries are made in the register in relation to personal data held for separate purposes, a separate request must be made and a separate fee may be paid by the individual in respect of each entry (*subsection (2)*). A data controller need not comply with a request for access if he is not satisfied about the identity of the individual making the request or has not been given enough information to enable the data to be traced (*subsection (3)*).

13. *Section 4 (4)* provides that a data controller will not be obliged to comply with a request for access if that would result in disclosing personal data about another individual unless that individual has consented to the disclosure. The data controller is not *prohibited* from disclosing the information, even if the other individual has not consented; he is merely not obliged to disclose it. However, the controller will be obliged to disclose so much of the information as he reasonably concludes can be supplied without thereby identifying the other individual to the data subject, e.g. by omitting names or other identifying particulars. The subsection applies only where the disclosure would identify an individual, as distinct from, say, a firm. (As stated, the operation of this provision, as well as of the other provisions conferring rights on data subjects, can be investigated by the Commissioner on receipt of a complaint — see *section 10 (1) (a).*).

14. *Section 4 (5)* is designed to prevent a data controller from amending personal data between the date the request for a copy of the data is received and the date the request is complied with but it permits amendments to be made that would have been made irrespective of the receipt of the request, e.g. details automatically added of further purchases made by the data subject during the period in question.

15. *Section 4 (6)* makes special provision in regard to requests for examination results. These requests are deemed to have been made on the date of the first publication of the results or on the date of the request, whichever is the later; and the period within which the examining authority is required to comply with requests is extended from 40 days to 60 days.

16. *Section 4 (7)* provides that a notification of a refusal of a request for access must include a statement of the reasons for the refusal and an indication that the data subject concerned may complain to the Commissioner about it.

17. *Section 4 (8)* empowers the Minister for Justice, if he considers it desirable to do so in the interests of data subjects and after consultation with the Minister for Health and other Ministers concerned, to make regulations modifying the right of access to personal data relating to physical or mental health or to social work, subject to such safeguards and to such extent as may be specified in the regulations.

18. ***Section 5*** provides for a number of restrictions on the right of access conferred by *section 4*. It also makes it clear that the provisions of the Bill authorising access to personal data override any existing enactment or rule of law prohibiting or restricting the disclosure of information or authorising it to be withheld. However, this will not apply in relation to any such enactment or rule of law if the Minister for Justice, after consultation with any other Minister concerned, considers that it should continue to prevail in the interests of the data subjects concerned or any other individuals and provides accordingly by regulations (*subsection (3)*).

19. *Section 5 (1)* sets out these restrictions on the right of access. They are either absolute, e.g. those for data covered by legal professional privilege or for back-up data, or those which apply only in specified circumstances, i.e. where disclosure would prejudice the prevention of crime, collection of taxes etc., prison security, the protection of the public against fraud, the protection of the international interests of the State or the interests of a data controller in relation to a claim against him or where, in the case of statistical or research data, the data do not disclose the identity of the data subjects concerned. (If a data subject considers that an exemption claimed is not justified in the particular circumstances of his case, a complaint can be made to the Commissioner.) *Paragraph (b)* of *subsection (1)* provides that data that are exempt from the right of access because access would prejudice the prevention of crime etc. will continue to be exempt if passed to a statutory body, e.g. the Garda Síochána Complaints Board, even if the data are not kept by that body for such purposes.

20. ***Section 6 (1)*** entitles a data subject to have personal data rectified or erased if they have been dealt with by a data controller in contravention of the provisions of *section 2 (1)*. A data controller is required to comply with a request for rectification or erasure within 40 days of being requested to do so. The controller is deemed to have complied with the request if, instead of rectifying or erasing the data, he supplements them with an agreed statement relating to the matters dealt with by the data; and, in that event, he will not, as respects those data, be in breach of the requirement of accuracy etc. provided for in *section 2 (1) (b)*. *Subsection (2)* requires a data controller who rectifies, erases or supplements data under this section to notify the rectification etc. not only to the data subject but also (if there has been a material modification of the data) to any person to whom the data were disclosed during the preceding twelve months.

21. ***Section 7*** provides that, to the extent that the law of torts does not already so provide, data controllers and data processors will owe

a duty of care to data subjects in collecting or dealing with personal data, that is, a duty to take reasonable care to prevent their activities in this respect causing damage to the data subjects concerned. However, a data controller will be deemed for the purposes of this section to have complied with the provisions of *section 2 (1) (b)* requiring data to be accurate and, where necessary, kept up to date if the data accurately record data or other information received or obtained from the data subject or a third party and if they include an indication to that effect and also a further indication, if such be the case, that the data subject has informed the data controller that he regards the data as inaccurate or not up to date, together with any supplementary statement provided pursuant to the Act (see proviso to *section 6 (1)* and also *section 10 (3)*).

22. A data controller will be in breach of the provisions of the Bill if he discloses personal data in any manner incompatible with the purposes for which they are kept or, where he is required to be registered under the Bill, if he discloses personal data to any person who is not described in the relevant entry in the register. However, ***section 8*** relieves data controllers in a number of cases from these restrictions on disclosure, e.g. where, in the opinion of a garda chief superintendent or an army colonel designated by the Minister for Defence, the disclosure is required for safeguarding the security of the State or where the disclosure is required for the prevention of crime etc. or is urgently required to prevent injury or other damage to the health of a person or serious damage to property etc. The section does not compel disclosure of the personal data concerned in the cases mentioned in it. A data controller is merely relieved from the restrictions on disclosure provided for by the Bill and he will still be subject to any such restrictions that may apply apart from those in the Bill.

The Data Protection Commissioner

General

23. *Sections 9* to *15* and the *Second Schedule* provide for the appointment by the Government of a Data Protection Commissioner (an Coimisinéir Cosanta Sonraí). The Commissioner will be independent in the exercise of his functions and will be empowered to enforce compliance with the provisions of the Bill dealing with the protection of personal data either on his own initiative or following complaints from data subjects. He will encourage the preparation and dissemination of codes of practice to govern various sectors of activity and will be the designated officer for the purpose of the mutual assistance provisions in the Convention. As part of his functions in relation to maintaining the register of data controllers and data processors to be established under *section 16,* he is being authorised to accept or refuse applications for registration or for the alteration or renewal of registrations. Under *section 20* he may, with the consent of the Minister for Justice, make regulations prescribing the procedure etc. to be followed in connection with registration.

24. ***Section 10*** empowers the Commissioner to deal with contraventions of the provisions of the Bill (other than provisions whose contravention would constitute an offence) by issuing an enforcement notice requiring the data controller or data processor concerned to take whatever steps are necessary to comply with those provisions (*subsection (2)*). Specific provision is made in *subsection (3)* for the Commissioner to require a data controller to rectify or erase personal data. In an appropriate case, the Commissioner may, instead of requiring rectification or erasure, require the data controller to supplement the data with a statement approved of by him. Where this is done, the data controller is deemed not to be in contravention of the

requirement of accuracy etc. provided for in *section 2 (1) (b)*. On complying with the requirement, the data controller must notify the data subject of the rectification etc. and also (if there has been a material modification of this data) any person to whom the data were disclosed during the period commencing twelve months before service of the enforcement notice *(subsection (7))*.

25. The enforcement notice will not have effect pending the determination of any appeal to the Circuit Court but in cases of urgency the Commissioner may require the notice to be complied with within the time specified in it, and that must be at least seven days from the date of its being served. In those cases, if the person concerned appeals within the specified time, the Court may determine whether the notice should have effect within that time or whether it should be extended to all or part of the period covered by the appeal proceedings (*section 26 (4)*). (Similar provision for such special circumstances is also made in relation to notices by the Commissioner prohibiting the transfer of personal data abroad *(section 11)* and notices requiring information to be furnished to the Commissioner *(section 12)*. Failure or refusal, without reasonable excuse, to comply with any of the requirements specified in these notices will be an offence.)

26. ***Section 11*** gives effect to article 12 of the Convention which is designed to reconcile the requirements of effective data protection with the desirability of facilitating international transfers of data. Accordingly the Commissioner, when considering whether to prohibit a proposed transfer of personal data to a place in a state bound by the Convention, must have regard to the provisions of article 12 (*subsection (2)*). That article provides that a contracting party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another party. Nevertheless, each party is entitled to derogate from this requirement in so far as its legislation includes specific regulations for certain categories of personal data because of their nature (e.g. health data), except where the regulations of the other party provide an equivalent protection. A derogation is also permissible if the transfer is to a non-contracting state through the intermediary of the territory of a contracting party in order to circumvent the specific regulations referred to.

27. *Section 11 (3)* deals with proposed transfers of personal data to states not bound by the Convention. The Commissioner must allow such transfers unless he is of opinion that it would lead to a contravention of the basic data protection principles set out in Chapter II of the Convention. In determining whether to prohibit any transfer of personal data the Commissioner must consider also whether the transfer would be likely to cause damage or distress to any person and have regard to the desirability of facilitating international transfers of data. The section does not apply to data the transfer of which is required or authorised by any enactment or required by any international agreement binding the State but it will apply to non-automated personal information transferred abroad for conversion into automated data.

28. ***Section 12*** empowers the Commissioner to require such information to be furnished to him as is necessary or expedient for the performance of his functions. Failure or refusal, without reasonable excuse, to comply with an information notice, or furnishing false or misleading information in purported compliance with it, will be an offence (*subsection (5)*). *Subsection (4)* provides that no enactment or rule of law prohibiting or restricting the disclosure of information shall preclude a person from furnishing to the Commissioner any

information that is necessary or expedient for the performance of his functions; but state security information or information that is privileged from disclosure in court proceedings, e.g. communications between a lawyer and client, are excluded from this provision.

29. ***Section 13*** requires the Commissioner to encourage the preparation of codes of practice by bodies representing data controllers or data processors and the dissemination of any such codes that he may approve of. Any such codes that are approved of by a resolution of each House of the Oireachtas will have the force of law.

30. ***Section 14*** provides for the Commissioner to prepare an annual report on his activities and to cause it to be laid before each House of the Oireachtas.

31. ***Section 15*** designates the Commissioner for the purposes of Chapter IV of the Convention. Article 13 in that Chapter makes provision for parties to render each other mutual assistance in order to implement the Convention and for each party to designate one or more authorities for that purpose. Designated authorities are obliged, on request, to give each other information on the law and administrative practice relating to data protection in their country. Articles 14 to 17 in Chapter IV set out the obligations undertaken by the parties towards one another, such as the rendering of assistance to data subjects resident abroad, the safeguards necessary as regards confidentiality in such circumstances, arrangements in regard to costs etc. *Subsection (2)* authorises the Minister for Justice to make any regulations that may be necessary or expedient to enable these mutual assistance provisions to have full effect.

Registration

General

32. The provisions under this heading — *sections 16* to *20* and the *Third Schedule* — require the Commissioner to establish and maintain a register of those categories of data controllers that are specified in the Bill or may subsequently be added under regulations made by the Commissioner with the consent of the Minister for Justice (*section 16 (1)*). Data processors who are in the business of processing personal data on behalf of data controllers must also register. The Commissioner is empowered to refuse applications for registration but he must do so where data controllers handle particularly sensitive data (e.g. relating to racial origin, health etc.) unless he considers that they are providing, and will continue to provide, appropriate safeguards for protecting the privacy of the individuals concerned *(section 17)*. It will be an offence for the specified data controllers or data processors to fail to register or for registered data controllers to deal with personal data otherwise than in accordance with the purposes etc. stated in the relevant entry in the register *(section 19)*.

33. ***Section 16 (1)*** lists those persons and bodies who are required to register. The data controllers concerned are: (a) those in the public sector, as listed in the *Third Schedule;* (b) financial institutions, insurance companies and agencies dealing with credit references, debt collecting, direct marketing and direct mailing; (c) those keeping personal data relating to racial origin, political opinions, religious or other beliefs, health, sexual life or criminal convictions, i.e. the special categories of data that in accordance with article 6 of the Convention may not be processed automatically unless domestic law provides adequate safeguards; and (d) such other categories as may be prescribed by the Commissioner with the consent of the Minister for Justice. (Data controllers will not however be obliged to register merely because they keep health data on their employees in the ordinary course of personnel administration and do not use or disclose

the data for any other purpose.) As stated, data processors who are in the business of processing data for others must also register. The register will be open to public inspection free of charge *(subsection (2))*.

34. ***Section 17*** requires applicants for registration to furnish whatever information the Commissioner may require and to pay the prescribed fee (*subsection (1)*). *Subsections (2)* and *(3)* distinguish between the approach to be adopted by the Commissioner in relation to applications concerning the particularly sensitive data mentioned in *section 16 (1) (c)* — data relating to racial origin etc. — and all other applications. In general, he will be obliged to accept applications unless he considers that the particulars supplied are insufficient or that the applicants are likely to contravene any of the provisions of the Bill. However, in the case of applications relating to the sensitive data referred to, he must refuse them unless he considers that appropriate safeguards for the protection of the privacy of the data subjects concerned are being, and will continue to be, provided by the applicants. Applicants are treated as registered until they receive a notification that their application has been accepted or refused or until they withdraw it, so that during that period they are not in breach of the prohibition in *section 19* on keeping personal data without being registered. In the case of a refusal, the period is extended for a further period of 21 days during which an appeal against the refusal can be brought and, if an appeal is brought, until the appeal is withdrawn or determined (*subsection (6)*). In special circumstances, that period can be reduced by the Commissioner to 7 days after the notification of refusal is received (*subsection (5)*) though it can be extended by the Circuit Court if an appeal is made to it within that period (*section 26 (4)*).

35. ***Section 18*** provides that a registration, or a registration that is continued, will be for a prescribed period of not less than one year.

36. ***Section 19*** makes it an offence for data controllers or data processors who are required by *section 16 (1)* to register to keep or process personal data without being registered. It will also be an offence for data controllers to take any action in relation to personal data that is at variance with their intentions as stated in the relevant entries in the register — for example, they may not keep or use data for a purpose not specified in the entry or disclose data to someone who is not described in the entry (other than to a person to whom a disclosure may be made under *section 8*). Obligations in this regard are also imposed on employees or agents of registered data controllers (*subsection (3)*). Registered persons or bodies are required to notify any change of address (*subsection (5)*).

37. ***Section 20*** authorises the Commissioner, with the approval of the Minister for Justice, to make regulations prescribing such matters as the procedure to be followed in applying for registration and any other matters that may be necessary or expedient to enable *sections 16* to *19* to have full effect.

Miscellaneous

38. ***Section 21*** makes it an offence for a data processor, or an employee or agent of his, knowingly to disclose personal data without the prior authority of the data controller on behalf of whom the data are processed.

39. ***Section 22*** makes it an offence for a person to obtain personal data without the prior authority of the data controller or processor concerned (by "hacking" or otherwise) and disclose it to another

person. To constitute the offence there must not only be unauthorised access to the data but a subsequent disclosure. The section does not apply to an employee or agent of the data controller or data processor concerned: a disclosure by an employee or agent of a registered data processor or data controller contrary to *section 19 (2) (d)* is an offence. Disclosures by unregistered data controllers or their employees or agents in breach of *section 2 (1) (c) (ii)* do not constitute an offence but may be made the subject of an enforcement notice.

40. ***Section 23*** provides that in general the Bill applies only to data controllers who control the contents and use of data from within the State and to data processors who process data on equipment located within the State *(subsections (1)* and *(2))*. There are two exceptions. *Subsection (3)* provides that, if a non-resident controls the contents and use of personal data within the State through an employee or agent in the State, the employee or agent is deemed to be acting on his own account and therefore to be subject to the provisions of the Bill. Second, the Bill will not apply to data wholly processed abroad for a resident in the State unless the data are used, or intended to be used, in the State (*subsection (4)*). *Subsection (5)* makes it clear that the prohibition in *section 19 (2) (e)* on a registered data controller transferring data to a place outside the State does not apply where the data are already outside the State, i.e. where the transfer is between places outside the State.

41. ***Section 24*** sets out various powers that may be exercised by an officer authorised by the Commissioner to obtain any information that is necessary or expedient for the performance by the Commissioner of his functions. These powers may not be exercised in relation to a financial institution without the prior sanction of the High Court (*subsections (3)* to *(5)*). It will be an offence to obstruct or impede an authorised officer or, without reasonable excuse, not to comply with a requirement of the officer or knowingly to give false or misleading information in purported compliance with such a requirement.

42. ***Section 25*** is a technical provision relating to service of notices.

43. ***Section 26*** provides for an appeal to the Circuit Court against decisions of the Commissioner. Jurisdiction is being given to the judge assigned to the circuit where the appellant ordinarily resides or carries on any profession, business or occupation or, at the option of the appellant, to a judge assigned to the Dublin circuit. An appeal may be brought to the High Court from a decision of the Circuit Court, but only on a point of law (*subsection (3)*). *Subsection (4)* deals with appeals made in cases where the Commissioner has decided that his decision should be complied with urgently. In those special cases the data controller concerned is obliged by the relevant provisions of the Bill to comply with the decision within the period specified by the Commissioner, whereas in the normal case he need not comply with it until any appeal against it is finally determined. This subsection allows the Court to extend the period specified for compliance in those cases either until the appeal is determined or withdrawn or for a shorter period, provided that the appeal has been brought within the specified period.

44. ***Section 27 (1)*** provides for the admissibility in evidence of certificates of the opinion of the Ministers for Justice and Defence, a garda chief superintendent or a designated army colonel (see *sections 1 (4) (a)*, *8 (a)* and *12 (4) (b)*). Under *subsection (2)* of the section information supplied by a person in compliance with a request by a data subject, a requirement under the Act or a direction of a court in proceedings under the Act will not be admissible in evidence against him or his spouse in proceedings for an offence under the Act.

45. ***Section 28*** provides that the whole or any part of proceedings under the Bill may be heard otherwise than in public.

46. ***Section 29*** is a standard provision. It provides that in certain circumstances directors etc. of a body corporate that commits an offence under the Bill are themselves also guilty of an offence.

47. ***Section 30*** authorises the Commissioner to bring summary proceedings for an offence under the Bill within a year from the date of the offence.

48. ***Section 31*** provides for a maximum fine of £1,000 on summary conviction of an offence under the Bill. The maximum fine on conviction on indictment is £50,000. The court is also being authorised to order the forfeiture or destruction of any data material connected with the offence or to have any relevant data erased. *Subsection (4)* is a standard provision, substituting the maximum fine of £1,000 provided by this section on summary conviction for the penalties provided in section 13 of the Criminal Procedure Act 1967 for indictable offences dealt with summarily under that section on a plea of guilty.

49. ***Sections 32, 33*** and ***34*** are routine provisions dealing with the laying of regulations before the Houses of the Oireachtas, fees under the Bill and the expenses incurred by the Minister in the administration of the Act.

50. ***Section 35*** contains the short title and commencement provisions. *Subsection (2)* allows the Minister for Justice by order to bring different provisions of the Bill into operation on different dates.

51. The *First Schedule* contains the text of the Convention and the *Second Schedule* the provisions concerning the Commissioner and his staff. The *Third Schedule* lists the public authorities and other bodies and persons required to register as data controllers pursuant to *section 16 (1) (b)* and provides for the addition of other data controllers in the public sector by regulations made by the Commissioner with the consent of the Minister for Justice.

An Roinn Dlí agus Cirt,
Iúil, 1988.

Wt. 160260/B/7. 1,225. 7/88. Cahill. (21532). G.16.