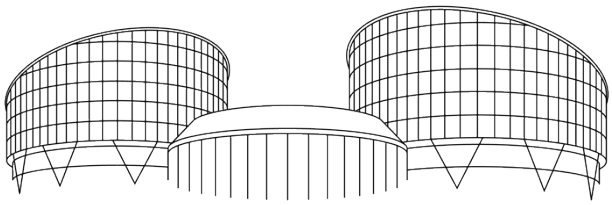

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FOURTH SECTION

CASE OF M.M. v. THE UNITED KINGDOM

(Application no. 24029/07)

JUDGMENT

STRASBOURG

13 November 2012

FINAL

29/04/2013

This judgment has become final under Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of M.M. v. the United Kingdom,

The European Court of Human Rights (Fourth Section), sitting as a Chamber composed of:

Lech Garlicki, *President,*
Nicolas Bratza,
Päivi Hirvelä,
George Nicolaou,
Ledi Bianku,
Nebojša Vučinić,
Vincent A. De Gaetano, *judges,*
and Lawrence Early, *Registrar,*

Having deliberated in private on 23 October 2012,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 24029/07) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a British national, Ms M.M. ("the applicant"), on 1 March 2007. The Vice-President of the Section granted the applicant anonymity (Rule 47 § 3 of the Rules of Court).

2. The applicant was represented by Mr B. Kennedy QC, a lawyer practising in Belfast. The United Kingdom Government were represented by their Agents, Ms H. Moynihan and Ms A. Sornarajah, of the Foreign and Commonwealth Office.

3. The applicant complained in particular about the retention and disclosure in the context of a criminal record check of data concerning a caution she received from the police.

4. On 5 October 2010 the application was communicated to the Government. It was also decided to rule on the admissibility and merits of the application at the same time (Article 29 § 1).

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

5. The applicant was born in 1951 and lives in County Tyrone, Northern Ireland.

6. In April 2000 the girlfriend of the applicant's son wished to leave Northern Ireland with the applicant's ten-month old grandson and return to live in Australia following her separation from the applicant's son. In order to try and force her son and his girlfriend to reconcile their differences, and in the hope that her grandson would not return to Australia, the applicant disappeared with her grandson at 6 p.m. on 19 April 2000 without the parents' permission. The police were called and the child was returned unharmed on the morning of 21 April 2000.

7. The applicant was subsequently arrested for child abduction. At a police interview on 24 April 2000, in the presence of her solicitor, the applicant confirmed that she had been aware at the time that she took her grandson that her conduct amounted to child abduction.

8. By letter dated 10 October 2000 the Director of Public Prosecutions recorded his decision that the public interest did not require the initiation of criminal proceedings against the applicant and that no such proceedings should therefore be brought. Instead, he indicated that a caution should be administered.

9. The applicant received a caution for child abduction which was formally administered on 17 November 2000.

10. On 6 March 2003, in reply to a query from the applicant, the police advised her that her caution would remain on record for five years, and so would be held on record until 17 November 2005.

11. On 14 September 2006 the applicant was offered employment as a Health Care Family Support Worker within Foyle Health and Social Services Trust ("the Trust") through Westcare Business Services ("Westcare"), subject to vetting. She was asked to disclose details of prior convictions and cautions. She accordingly disclosed details of the incident of April 2000 and her subsequent caution on the form provided, and consented to a criminal record check. Westcare contacted the Criminal Records Office of the Police Service of Northern Ireland ("Criminal Records Office") to verify the details disclosed. The existence of the caution was duly verified.

12. On 31 October 2006 Westcare withdrew the offer of employment, indicating that it had taken into account the verification by the Criminal Records Office of the caution for child abduction.

13. The applicant subsequently sought to challenge her acceptance of the caution in November 2000 by letter to the Criminal Records Office. In an undated letter, the Criminal Records Office replied to her in the following terms:

> "... in a case where someone agrees to be cautioned by the police for a particular offence, by doing so they are accepting that they were guilty of the offence in the first place. This information is printed on the caution form, which you signed on 17th November 2000.

Regrettably there is no way to change that. The case cannot be brought back to a court because the whole idea of the caution was to keep it out of court in the first instance.

I should also point out that the information given to Sgt Dunne and which he relayed to you in 2003, about the weeding date for an adult caution, was correct at that time but there has since been a policy change. Normally an adult caution will be weeded after a period of five years, provided the defendant has not been convicted of any further offences. However following the murder of the schoolgirls in Soham England and the subsequent Bichard Report the weeding policy was changed in relation to all cases where the injured party is a child. The current policy is that all convictions and cautions, where the injured party is a child, are kept on the record system for life."

14. The letter concluded:

"I fully appreciate that the offence in your case was not the normal type of offence and that the child did not suffer any harm and that it was never your intention that he should suffer any harm. The offence code under which the offence comes for computing purposes classes the offence as 'child abduction' (by other person). Which means a person other than a parent of the child.

... Perhaps you would be good enough to contact me ... in order that we might discuss the matter and perhaps find some means of ameliorating the consequences of the information given above."

15. By letter dated 6 May 2006 to the applicant's solicitor, the Criminal Records Office confirmed that in signing the caution form the applicant had accepted guilt for the offence in question and that nothing could be done to change the criminal record. The applicant's solicitor subsequently informed her that there did not appear to be any action which she could take in relation to the removal of the caution.

16. By letter dated 6 December 2006 Detective Superintendent Thomson of the Northern Ireland Police Service confirmed that he would not delete the caution from police records. However he proposed, with the applicant's agreement, to add a comment to the effect that the incident was domestically related and that in any vetting context the applicant should be approached for an explanation.

17. In January 2007 the Northern Ireland Legal Services Commission ("the LSC") refused an application for legal aid, made by the applicant's solicitor, to review the Trust's decision not to employ the applicant. The solicitor informed the applicant that she could appeal the LSC's decision at a cost of GBP 500 for representation by counsel, but the applicant could not afford to instigate legal proceedings without public funding.

18. In February 2007 the applicant was interviewed for a position as a Family Support Worker. The interview letter advised that the position was a regulated one under Article 31 of the Protection of Children and Vulnerable Adults (Northern Ireland) Order 2003 and she was asked to complete a consent form and bring it to the interview.

19. On 29 March 2007 the applicant was informed that her application for the position was unsuccessful. No reasons were provided.

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. The aims and nature of a caution

20. At the relevant time the purpose of a formal caution was set out in Police Force Order no. 9/96 issued by the Royal Ulster Constabulary, namely:

> "(a) to deal quickly and simply with less serious offenders;
>
> (b) to divert offenders in the public interest from appearance in the criminal courts; and
>
> (c) to reduce the likelihood of re-offending."

21. The Order further noted:

> "... a formal caution is not a form of sentence ...
>
> (a) A formal caution is nonetheless a serious matter. It is recorded by police; it may be relevant in relation to future decisions as to prosecution, and it may be cited in any subsequent criminal prosecutions. Properly used, caution is an effective form of disposal.
>
> ..."

B. Retention of conviction and caution data in police records

1. The statutory background

22. Article 29(4) of the Police and Criminal Evidence (Northern Ireland) Order 1989 (as subsequently amended) provides that:

> "... the Secretary of State may by regulations make provision for recording in police records convictions for such offences as are specified in the regulations."

23. The regulations made by the Secretary of State under this provision are the Northern Ireland Criminal Records (Recordable Offences) Regulations 1989. These regulations identify the relevant convictions as being those for offences punishable by imprisonment, as well as a number of additional specified offences. The regulations do not make any reference to cautions.

24. According to the Government, the recording of cautions in Northern Ireland takes place under the police's common law powers to retain and use information for police purposes. That power is subject to the provisions of the Data Protection Act 1998 (see generally paragraphs 65-71 below).

2. Policy and practice

(a) The policy and practice of the Police Service in Northern Ireland

25. According to the Government, the policy and practice of the Police Service in Northern Ireland ("PSNI") at the time of the issue of the applicant's caution in 2000 was to delete cautions from the individual's criminal record after five years.

26. However, following publication of the Bichard Report in 2006 (see paragraphs 31-32 below), the PSNI changed its practice so as to retain information on adult cautions for the rest of a person's life.

(b) Relevant policy documents

(i) The ACPO Codes of Practice of 1995, 1999 and 2002

27. The chief constable of PSNI is a member of the Association of Chief Police Officers of England and Wales and Northern Ireland ("ACPO").

28. Pursuant to the ACPO Code of Practice 1995 ("the 1995 ACPO Code"), in cases of conviction for an offence that carried the possibility of imprisonment, a record of the conviction had to be retained for a period of twenty years. Exceptions to this included cases where the conviction was for an offence against a child or young person, where the record was to be retained until the offender was 70 years old, subject to a minimum 20-year retention period; and cases involving rape, where the record was to be retained for the life of the offender.

29. Records of cautions (assuming there were no other convictions or further cautions) were to be retained for a five-year period.

30. The 1995 ACPO Code was updated in 1999 and subsequently replaced by another code of practice in 2002. Neither instrument substantially altered the provisions regarding retention of data relating to cautions.

(ii) The Bichard Inquiry Report 2004

31. Following the murders of two young girls in August 2002 by a caretaker employed at a local school, a review of the United Kingdom's police forces was announced by the Home Secretary. An inquiry was set up, to be conducted by Sir Michael Bichard.

32. The Bichard Inquiry Report ("the Bichard report") was published in June 2004. It reviewed current practice as regards retention of data on

convictions and cautions and concluded (at paragraph 4.41) that "there were a number of problems with the review, retention or deletion of records." The report recommended that:

> "A Code of Practice should be produced covering record creation, review, retention, deletion and information sharing. This should be made under the Police Reform Act 2002 and needs to be clear, concise and practical. It should supersede existing guidance."

(iii) Code of Practice on the Management of Police Information 2005

33. In July 2005 the Secretary of State adopted a Code of Practice on the Management of Police Information ("the 2005 Code of Practice"). The Code applies directly to police forces in England and Wales and is available for adoption by other police forces. The Government did not clarify whether the Code has been adopted by the PSNI.

34. Paragraph 1.1.1 of the Code explains that police forces have a duty to obtain and use a wide variety of information, including personal information. The Code clarifies that responsibility for the management and use of information lies with the chief officer of the police force. It recognises the existing legislative framework for the management of information relating to data protection and human rights set out in the Data Protection Act (see paragraph 65-71 below).

35. The Code sets out a number of key principles including, *inter alia*, the duty to obtain and manage information; the importance of recording information considered necessary for a police purpose; and the need to review information and consider whether its retention remains justified, in accordance with any guidance issued.

(iv) Guidance on the Management of Police Information 2006 and 2010

36. In 2006 ACPO published Guidance on the Management of Police Information. This Guidance was applied by the PSNI. A second edition was published in 2010 ("the MOPI Guidance"), and is also applied by the PSNI.

37. Chapter 7 of the MOPI Guidance deals with review, retention and disposal of police information not contained on the Police National Computer ("PNC"). The PNC is the system for recording conviction data in England and Wales; the Causeway system is used in Northern Ireland. The MOPI Guidance notes at the outset that:

> "7.2.1 ... Public authorities, including police forces, must act in a way that complies with the European Convention on Human Rights (ECHR) and the Human Rights Act 1998. In relation to record retention this requires a proportionate approach to the personal information held about individuals. The decision to retain personal records should be proportionate to the person's risk of offending, and the risk of harm they pose to others and the community. A higher proportionality test should be met in order to retain records about relatively minor offending."

38. The MOPI Guidance also refers to the need to comply with the principles of the Data Protection Act (see paragraph 65-71 below).

39. The MOPI Guidance sets out the framework for decision-making in respect of retention of police information. It provides that records should be kept for a minimum period of six years, beyond which time there is a requirement to review whether retention of the information remains necessary for a policing purpose. Relevant questions are whether there is evidence of a capacity to inflict serious harm, whether there are concerns relating to children or vulnerable adults, whether the behaviour involved a breach of trust, whether there is evidence of links or associations which might increase the risk of harm, whether there are concerns as to substance misuse and whether there are concerns that an individual's mental state might increase the risk. In any review, the MOPI Guidance notes that there is a presumption in favour of retention of police information provided that it is not excessive, is necessary for a policing purpose, is adequate for that purpose and is up to date.

40. The MOPI Guidance also contains a review schedule based on the seriousness of offences. Under the review schedule, information is divided into four categories. Group 1 is called "Certain Public Protection Matters", which includes information relating to individuals who have been convicted, acquitted, charged, arrested, questioned or implicated in relation to murder or a serious offence as specified in the Criminal Justice Act 2003 (or historical offences that would be charged as such if committed today). Such information should only be disposed of if it is found to be entirely inaccurate or no longer necessary for policing purposes. The MOPI Guidance continues:

> "Forces must retain all information relating to certain public protection matters until such time as a subject is deemed to have reached 100 years of age (this should be calculated using the subject's date of birth). There is still a requirement, however, to review this information regularly to ensure that it is adequate and up to date. This must be done every ten years ...
>
> Due to the seriousness of this group, no distinction is made between the type or classification of information that can be retained for 100 years; information retained under this grouping can include intelligence of any grading.
>
> There may be extreme cases where the retention of records relating to certain public protection matters would be disproportionately injurious to the individual they are recorded against. For example, an individual arrested on suspicion of murder for a death that is subsequently found to have been the result of natural causes, or an entirely malicious accusation that has been proven as such, would both generate records that can only be adequate and up to date if they reflect what actually happened. Particular care must be exercised in disclosing any such records to avoid unnecessary damage to the person who is the subject of the record."

41. The other categories are "Other Sexual, Violent or Serious Offences (Group 2), in respect of which information should be retained for as long as

the offender or suspected offender continues to be assessed as posing a risk of harm; "All Other Offences" (Group 3), in respect of which police forces may choose to use a system of time-based, automatic disposal if it is considered that the risk of disposal is outweighed by the administrative burden of reviewing the information or the cost of retaining it; and "Miscellaneous" (Group 4), which covers a variety of other cases and entails different guidance on retention in each one.

(v) Retention Guidelines for Nominal Records on the Police National Computer 2006

42. The ACPO Retention Guidelines for Nominal Records on the Police National Computer 2006 ("the ACPO Guidelines") came into effect on 31 March 2006. The ACPO Guidelines form part of the guidance issued under the MOPI Code and are applied by PSNI.

43. The ACPO Guidelines explain that:

> "1.3 The Retention Guidelines are based on a format of restricting access to PNC data, rather than the deletion of that data. The restriction of access is achieved by setting strict time periods after which the relevant event histories will 'step down' and only be open to inspection by the police. Following the 'step down' other users of PNC will be unaware of the existence of such records, save for those occasions where the individual is the subject of an Enhanced Check under the Criminal Records Bureau vetting process ... "

44. They continue:

> "2.8 ...the Nominal records will now contain 'Event Histories' to reflect the fact that the subject may have been Convicted (including cautions, reprimands and warnings), dealt with by the issue of a Penalty Notice for Disorder, Acquitted, or dealt with as a 'CJ Arrestee' [a person who has been arrested for a recordable offence under the Criminal Justice Act 2003 but in respect of whom no further action was taken]."

45. The general principle set out in paragraph 3.1 of the ACPO Guidelines is that when a nominal record is created or updated on the PNC by virtue of an individual being convicted, receiving a Penalty Notice for Disorder, being acquitted or being a CJ Arrestee, the record will contain the relevant personal data together with details of the offence which resulted in the creation of the record. The record will be retained on PNC until that person is deemed to have attained 100 years of age.

46. Paragraph 4.32 of the ACPO Guidelines clarifies that chief officers are the "data controllers" (within the meaning of the Data Protection Act 1998 – see paragraphs 65-71 below) of all PNC records, including DNA and fingerprints associated with the entry, created by their forces and that they have the discretion in exceptional circumstances to authorise the deletion of any such data. Appendix 2 of the ACPO Guidelines outlines the procedure to be followed in deciding whether a particular case will be regarded as "exceptional" and states:

"Exceptional cases by definition will be rare. They might include cases where the original arrest or sampling was found to be unlawful. Additionally, where it is established beyond reasonable doubt that no offence existed, that might, having regard to all the circumstances, be viewed as an exceptional circumstance."

C. Disclosure of a caution

1. The legal framework

(a) Prior to 1 April 2008

47. According to the Government, from the date on which the caution was administered to the applicant until 1 April 2008, requests for disclosure of criminal record data in Northern Ireland were made on a consensual basis. Disclosure took place in accordance with well-established common law powers of the police for police purposes only.

(b) After 1 April 2008

48. Part V of the Police Act 1997 ("the 1997 Act") now sets out the legislative framework for the disclosure of criminal record information in Northern Ireland. The relevant provisions entered into force in Northern Ireland on 1 April 2008.

49. Section 113A deals with criminal record certificates ("CRCs"). Section 113A(3) defines a CRC as follows:

"A criminal record certificate is a certificate which–

(a) gives the prescribed details of every relevant matter relating to the applicant which is recorded in central records, or

(b) states that there is no such matter."

..."

50. Section 113A(6) defines "central records" as such records of convictions and cautions held for the use of police forces generally as may be prescribed. In Northern Ireland, the relevant records are prescribed in the Police Act 1997 (Criminal Record) (Disclosure) Regulations (Northern Ireland) 2008 as information in any form relating to: convictions held in the criminal history database of the Causeway System; and convictions and cautions on a names index held by the National Police Improvement Authority for the use of police forces generally. The term "relevant matter" is defined in section 113A(6) of the 1997 Act as including "spent" convictions and cautions (see paragraphs 61-64 below). Pursuant to section 65(9) of the Crime and Disorder Act 1998 , the reference to a "caution" in section 113A is to be construed as including warnings and reprimands.

51. The Secretary of State must issue a CRC to any individual who makes an application in the prescribed manner and form and pays the prescribed fee. The application must be countersigned by a registered person and accompanied by a statement by the registered person that the certificate is required for the purposes of an exempted question. Section 113A(6) defines "exempted question" as follows: in respect of a conviction, a question which the Secretary of State has by order excluded from the provisions on "spent" convictions under the 1974 Act or the 1978 Order; and in respect of a caution, a question which the Secretary of State has by order excluded from the provisions on "spent" cautions under the 1974 Act; as noted above there is no corresponding provision in Northern Ireland. In respect of Northern Ireland, the Secretary of State subsequently made an order excluding the provisions on "spent" convictions in relation to questions directed, *inter alia*, at assessing the suitability of persons to work with children and vulnerable adults.

52. Section 113B deals with enhanced criminal record certificates ("ECRCs"). As with a CRC, the Secretary of State must issue an ECRC to any individual who makes an application in the prescribed manner and form and pays the prescribed fee. The application must be countersigned by a registered person and accompanied by a statement by the registered person that the certificate is required for the purposes of an exempted question asked for a "prescribed purpose".

53. The "prescribed purposes" are defined in the Police Act 1997 (Criminal Records) (Disclosure) Regulations (Northern Ireland) 2008 as amended and include the purposes of considering the applicant's suitability to engage in any activity which is regulated activity relating to children or vulnerable adults, as defined in legislation.

54. Section 113B(3) provides:

> "An enhanced criminal record certificate is a certificate which–
>
> (a) gives the prescribed details of every relevant matter relating to the applicant which is recorded in central records and any information provided in accordance with subsection (4), or
>
> (b) states that there is no such matter or information."

55. Section 113B(4) provides that before issuing an ECRC the Secretary of State must request the chief officer of every relevant police force to provide any information which, in the chief officer's opinion, might be relevant for the "prescribed purpose" and ought to be included in the certificate.

56. Pursuant to section 113B(5), the Secretary of State must also request the chief officer of every relevant police force to provide any information which, in the chief officer's opinion, might be relevant for the "prescribed purpose", ought not to be included in the certificate in the interests of the

prevention or detection of crime but can, without harming those interests, be disclosed to the registered person.

57. The Secretary of State must send to the registered person who countersigned the application a copy of the enhanced criminal record certificate, and any information provided in accordance with subsection (5).

2. Policy and practice

58. The MOPI Guidance explains the circumstances in which police information will be disclosed:

> "6.3.1. ... The Police Act 1997 creates a statutory scheme for the disclosure of criminal records and police information on potential employees to prospective employers. The CRB is responsible for the scheme and for ensuring that employers have sufficient information to make a judgment on the suitability of a potential employee to work with children or vulnerable adults."

59. The Guidance further refers to the possibility of sharing information under common law powers. In such cases, a policing purpose must be established and the decision to disclose data must strike a balance between the risk posed and the need for confidentiality of data under the Human Rights Act and the Data Protection Act.

60. As noted above, the ACPO Guidelines work on the basis of restricting access to police information rather than deleting data. Recordable offences are split into categories "A", "B" and "C" depending on the seriousness of the offence, with category A being the most serious offences. These categories mirror Groups 1, 2 and 3 set out in the MOPI Guidance. The Guidelines set strict time periods after which relevant data will "step down" and only be open to inspection by the police. The aim is to ensure that following step down, other users of the PNC will be unaware of the existence of the relevant records, save in cases of requests for criminal record checks. For example, the ACPO Guidelines state, at paragraph 4.19, that:

> "4.19 In the case of an adult who is dealt with by way of a caution in respect of an offence listed in category 'A', the conviction history will 'step down' after a clear period of 10 years, and thereafter only be open to inspection by the police."

D. Rehabilitation of offenders

61. Pursuant to legislation, those convicted of certain offences may become "rehabilitated" after a certain period of time has elapsed. The relevant legislation in England and Wales is the Rehabilitation of Offenders Act 1974 ("the 1974 Act"). The legislation which applies in Northern Ireland is the Rehabilitation of Offenders (Northern Ireland) Order 1978 ("the 1978 Order").

62. Pursuant to the 1978 Order, any person who has been convicted of an offence capable of rehabilitation and has not committed any other offence during the rehabilitation period is to be treated as rehabilitated at the end of the rehabilitation period.

63. The effect of rehabilitation is that the person is treated for all purposes in law as a person who has not committed, or been charged with, prosecuted for or convicted of the offence in question, i.e. the conviction is considered "spent". If asked about previous convictions, a person is to treat the question as not relating to spent convictions and may frame his answer accordingly; he is not to be liable or prejudiced for his failure to acknowledge or disclose a spent conviction. Spent convictions are not a proper ground for dismissing or excluding a person from employment. However, the Secretary of State is empowered to provide for exclusions, modifications or exemptions from the provisions on the effect of rehabilitation.

64. The 1978 Order makes no reference to cautions. However, the 1974 Act (which does not apply in Northern Ireland) contains a Schedule introduced in 2008 which provides protection for spent cautions. According to Schedule 2, a caution is to be considered a spent caution at the time that it is given. The effects of rehabilitation in respect of a caution are the same as those described above which apply to a conviction. As with convictions, the Secretary of State may, by order, provide for exclusions or exemptions.

E. The Data Protection Act 1998

65. The Data Protection Act ("the DPA 1998") was adopted on 16 July 1998. The main provisions of the Act entered into force on 1 March 2000.

66. The Act stipulates that the processing of personal data is subject to eight data protection principles listed in Schedule 1.

67. Pursuant to section 1 of the DPA 1998, "personal data" includes data which relate to a living individual who can be identified from those data. Section 2 of the Act defines "sensitive personal data" as personal data consisting, *inter alia*, of information as to the commission or alleged commission by him of any offence, or 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.

68. Under the first principle personal data shall be processed fairly and lawfully and, in particular shall not be processed unless (a) at least one of the conditions in Schedule 2 is met; and (b) in case of sensitive personal data, at least one of the conditions in Schedule 3 is also met. Schedule 2 contains a detailed list of conditions, including that the processing of any personal data is necessary for the administration of justice or for the exercise of any other functions of a public nature exercised in the public interest by any person (paragraphs 5(a) and (d)). Schedule 3 contains a more

detailed list of conditions, including that the processing is necessary for the purposes of performing an obligation imposed by law on the data controller in connection with employment (paragraph 1), the processing is necessary for the purpose of, or in connection with, any legal proceedings or is otherwise necessary for the purposes of establishing, exercising or defending legal rights (paragraph 6), or is necessary for the administration of justice or for the exercise of any functions conferred on any person by or under an enactment (paragraph 7). Section 29 provides a qualified exemption from the first data protection principle in the case of personal data processed, *inter alia*, for the prevention or detection of crime.

69. The third principle provides that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

70. The fifth principle stipulates that personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

71. The Information Commissioner created pursuant to the Act has an independent duty to promote the following of good practice by data controllers and has power under section 40 of the Act to make orders ("enforcement notices") in this respect. Section 47 of the Act makes it a criminal offence not to comply with an enforcement notice. Section 48 of the Act gives data controllers the right to appeal against an enforcement notice to the First Tier Tribunal, if an enforcement notice raises a point of law. Section 13 sets out a right to claim damages in the domestic courts in respect of contraventions of the Act.

F. The Human Rights Act 1998

72. Section 3(1) of the Human Rights Act 1998 ("the Human Rights Act") provides as follows:

> "So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights."

73. Section 4 of the Act provides:

> "(1) Subsection (2) applies in any proceedings in which a court determines whether a provision of primary legislation is compatible with a Convention right.
>
> (2) If the court is satisfied that the provision is incompatible with a Convention right, it may make a declaration of that incompatibility.
>
> ..."

74. Section 6(1) of the Act provides that it is unlawful for a public authority to act in a way which is incompatible with a Convention right. Section 6(2) clarifies that:

> "Subsection (1) does not apply to an act if–

(a) as the result of one or more provisions of primary legislation, the authority could not have acted differently; or

(b) in the case of one or more provisions of, or made under, primary legislation which cannot be read or given effect in a way which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions."

75. Section 7(1) provides that a person who claims that a public authority has acted in a way made unlawful by section 6(1) may bring proceedings against the authority.

76. Section 8(1) of the Act permits a court to make a damages award in relation to any act of a public authority which the court finds to be unlawful.

G. Judicial consideration

1. R (X) v Chief Constable of the West Midlands Police *[2004] EWCA Civ 1068*

77. In *R (X)*, the Court of Appeal considered the compatibility with Article 8 of the Convention of the disclosure of additional information under the predecessor of section 113B(4) of the 1997 Act in the context of an enhanced criminal records check. The appellant had applied for a job as a social worker and had no previous convictions. He had been charged with indecent exposure, but the proceedings were discontinued when the alleged victim failed to identify him. The social work agency which was dealing with his job application applied for an ECRC. The chief constable, as he was required to do, issued an ECRC. It contained details of the allegations of indecent exposure under the heading "other relevant information".

78. Lord Woolf CJ noted at the outset that while it was accepted by both parties that the information included in the ECRC might offend against Article 8 § 1, it was not suggested that the legislation itself contravened that Article. He explained:

"20. ... No doubt this is because disclosure of the information contained in the certificate would be 'in accordance with the law' and 'necessary in a democratic society', in the interests of public safety and for the prevention of crime and for the protection of the rights and freedoms of others. This country must, through its legislature, be entitled to enable information to be available to prospective employers, where the nature of the employment means that particular care should be taken to ensure that those who are working with the appropriate categories of persons can be relied on to do so, without those in their care coming to harm if they are under the age of 18 or vulnerable adults."

79. On the question of the balance between competing interests, Lord Woolf CJ indicated (at paragraph 36) that:

> "Having regard to the language of section 115 [the predecessor of section 113B], the Chief Constable was under a duty to disclose if the information might be relevant, unless there was some good reason for not making such a disclosure."

80. He continued (at paragraph 37):

> "This was obviously required by Parliament because it was important (for the protection of children and vulnerable adults) that the information should be disclosed even if it only might be true. If it might be true, the person who was proposing to employ the claimant should be entitled to take it into account before the decision was made as to whether or not to employ the claimant. This was the policy of the legislation in order to serve a pressing social need. In my judgment it imposes too heavy an obligation on the Chief Constable to require him to give an opportunity for a person to make representations prior to the Chief Constable performing his statutory duty of disclosure."

81. On the application of Article 8, assuming that it was engaged, he noted (at paragraph 41):

> "... [H]ow can the Chief Constable's decision to disclose be challenged under article 8? As already indicated, the Chief Constable starts off with the advantage that his statutory role is not in conflict with article 8, because the statute meets the requirements of article 8(2). It follows also, that as long as the Chief Constable was entitled to form the opinion that the information disclosed might be relevant, then absent any untoward circumstance which is not present here, it is difficult to see that there can be any reason why the information that 'might be relevant', ought not to be included in the certificate. I accept that it is possible that there could be cases where the information should not be included in the certificate because it is disproportionate to do so; the information might be as to some trifling matter; it may be that the evidence made it so unlikely that the information was correct, that it again would be disproportionate to disclose it. These were not, in my judgment, the situations on the facts before the Chief Constable."

2. R (R) v Durham Constabulary and another [2005] UKHL 21

82. The case of *R (R)* concerned the issue of a "reprimand or warning" to a young person for alleged offences of indecent assault. Unlike the issue of a caution, the issue of a reprimand or warning did not require the person's consent. However, like a caution, the issue of a reprimand/warning required the individual to admit to the offence. The issue of the reprimand/warning in the case had given rise to an obligation that the young offender in question be subject to registration pursuant to the Sex Offenders Act 1977. The claimant alleged that the reprimand had violated Article 6 of the Convention because it had been issued without his consent and the consequences of its issue, including the need to register on the Sex Offender Register, had not been properly identified to him.

83. The House of Lords unanimously rejected the claim. Lord Bingham of Cornhill doubted whether Article 6 had been engaged at all, but even assuming that it was, he concluded that it had ceased to apply once the decision had been made not to prosecute the claimant. He noted that there was little case-law from this Court as to the meaning of "determination" of

criminal charges and expressed the view that the determination of a criminal charge, to be properly so regarded, must expose the subject of the charge to the possibility of punishment, whether in the event punishment was imposed or not. He considered therefore that a process which could only culminate in measures of a preventative, curative, rehabilitative or welfare-promoting kind would not ordinarily involve the determination of a criminal charge. He accordingly concluded that neither the warning of the claimant nor the decision to warn him involved the determination of a criminal charge against him. Had they done so, Lord Bingham noted, it was acknowledged by the police force that there had been no valid waiver by him of his fair trial right.

3. R (S) v Chief Constable of West Mercia and Criminal Records Bureau [2008] EWHC 2811 (Admin)

84. The claimant challenged the inclusion under section 113B(4) of the 1997 Act of other information provided by the chief constable on an ECRC regarding alleged offences of which he had been found not guilty.

85. The High Court upheld the challenge and quashed the decision on the basis that the decision-maker had not taken reasonable steps to ascertain whether the allegations that had been made had been true and why the claimant had been acquitted. On the facts of the case it was clear that the Magistrates' Court had acquitted the claimant because it took the view that he was innocent in the full sense of the word. The High Court observed:

> "I stress, however, that this decision is very specific to the facts of this case. I do not suggest for one minute that allegations should not be disclosed in an ECRC simply because the alleged offender has been acquitted. The circumstances surrounding the acquittal are all important. There will be instances where an alleged offender is acquitted but only because the Magistrates (or Jury) entertain a reasonable doubt about the alleged offender's guilt. The tribunal of fact may harbour substantial doubts. In such circumstances, however, it might well be perfectly reasonable and rational for a Chief Constable to conclude that the alleged offender might have committed the alleged offence ..."

4. R (Pinnington) v Chief Constable of Thames Valley Police [2008] EWHC 1870 (Admin)

86. The Divisional Court considered a claim by an individual aggrieved by the disclosure in an ECRC of three allegations of sexual abuse of autistic persons in his care, where he had been interviewed by the police about one of the allegations but no charges were pursued.

87. The judge conducted a detailed analysis of the allegations and concluded:

> 58. It follows that in my judgment the decision to disclose the three allegations was lawful ... I recognise how painful such disclosure must be for the claimant, and how damaging its consequences may be. It seems to me, however, that all this follows

inevitably from the terms of the legislation and is fully in line with the legislative policy as explained by Lord Woolf *in R (X) v Chief Constable of the West Midlands Police*. In relation to employment with children or vulnerable adults, it is information of which an employer should be aware. It is then for the employer to decide whether the employment of the person concerned involves an unacceptable risk.

59. I am troubled by the fact that the claimant's new employer in this case apparently operated a blanket policy of insisting on a 'clean' certificate, so that the disclosure of the three allegations led inevitably to the claimant's dismissal on the transfer of his employment to that employer on a reorganisation at work. The legislation imposes a relatively low threshold for disclosure in the certificate in order to enable an employer to make a properly informed decision. But it is important that employers understand how low that threshold is and the responsibility that it places in practice upon them. A properly informed decision requires consideration not only of the information disclosed in the certificate but also of any additional information or explanation that the employee may provide. The operation of a blanket policy of insisting on a 'clean' certificate leaves no room for taking into account what the employee may have to say. That is a matter of particular concern if it leads to the dismissal of an existing employee or of someone whose employment is transferred to the employer on a reorganisation. On the basis of the limited material available to the court, I confess to some surprise that the claimant was advised in this case that he had no reasonable prospect of success in a claim for unfair dismissal resulting from the application of such a policy ..."

5. Chief Constable of Humberside & Others v The Information Commissioner & Another [2009] EWCA Civ 1079

88. The question for examination by the Court of Appeal in its judgment handed down on 19 October 2009 was whether certain principles of the Data Protection Act 1998, namely principle 1 (personal data shall be processed fairly and lawfully), principle 3 (personal data shall be adequate relevant and not excessive) and principle 5 (personal data shall not be kept for longer than necessary), required the police to delete certain old convictions from the PNC. Lord Justice Waller noted at the outset:

"1. ... The complaint in each case follows the disclosure of the convictions pursuant to a request by the ... CRB ... or, in one case, a request by one of the individuals herself, and it is important to emphasise at the outset that the complaint about retention flows in reality not from the retention itself but from the fact that, if retained, disclosure may follow. In respect of each of those convictions the Information Tribunal (the IT) has upheld the view of the Information Commissioner (the IC) that they should be deleted. However the ramifications are far wider than these five cases since, if these convictions must be deleted and if the police are to treat people consistently, the application of any viable system of weeding would probably lead to the deletion of around a million convictions."

89. He clarified the effect of the "stepping down" policy on disclosure in the context of criminal records checks, noting:

"3. ... [I]t seems that both the Police and the IT understood that the result of stepping down would be that in certain circumstances the CRB would not have access to 'stepped down' convictions when preparing 'standard disclosure certificates' (as

opposed to 'enhanced disclosure certificates') under Part V of the Police Act 1997. It is now accepted that that is not accurate. Under Part V of the 1997 Act 'stepped down' convictions are required to be revealed even on 'standard disclosure certificates', and thus although 'stepping down' prevents disclosure in many circumstances to persons other than the police, it does not prevent disclosure by the police in many others including the circumstances under which disclosure was made of four of the convictions the subject of this appeal."

90. Waller LJ noted that PNC information was used for employment vetting. He observed that CRCs and ECRCs would contain details of spent convictions which, he indicated, provided an important protection to employers. He noted:

"... Some emphasis is placed by [counsel for the intervenor] that no statutory obligation is placed on the police to retain data under the Police Act 1997, but on any view Part V of the Act seems to recognise that the data will be there to be provided."

91. Taking as an example the case of one of the individuals concerned, Waller LJ considered the purposes for which the data had been recorded:

"35. ... [I]t seems to me to be clear that one of the purposes for which the police retained the data on the PNC was to be able to supply accurate records of convictions to the CPS, the courts and indeed the CRB. 'Rendering assistance to the public in accordance with force policies' clearly covers the roles the police seek to perform in those areas and if there was any doubt about it the recipients include 'Employers' 'the courts' and 'law enforcement agencies'."

92. He continued:

"36. If one then poses the question whether the Data being retained is excessive or being retained for longer than necessary for the above purposes there is, it seems to me, only one answer, since for all the above a complete record of convictions spent and otherwise is required. That seems to me to be a complete answer to the appeal ..."

93. Even if a narrower approach to police purposes were adopted, Waller LJ considered that the retention of the data was lawful under the DPA 1998. He noted:

"43. ... If the police say rationally and reasonably that convictions, however old or minor, have a value in the work they do that should, in effect, be the end of the matter ... It is simply the honest and rationally held belief that convictions, however old and however minor, can be of value in the fight against crime and thus the retention of that information should not be denied to the police."

94. He continued:

"44. I emphasise the word 'retention' because if there is any basis for complaint by the data subjects in this case, it seems to me to relate to the fact that in certain circumstances this information will be disclosed, but that is because Parliament has made exceptions to the Rehabilitation of Offenders Act. What is more, the circumstances in which there will be disclosure are circumstances in which the Data Subject would be bound to give the correct answer if he or she were asked. It is not as it seems to me the purpose of the 1998 [Data Protection] Act to overrule the will of Parliament by a side wind."

95. As to the complaint of one of the individuals concerned, S.P., that she had been assured in 2001 that the reprimand she had received aged thirteen would be removed from her record when she was eighteen if she did not get into anymore trouble and that the retention of the reprimand on the PNC after her eighteenth birthday was therefore unfair under the first data protection principle, Waller LJ, with whom Lord Justice Hughes agreed, held:

> "48. ... It seems to me that if it is fair to retain convictions under the new policy it does not become unfair to do so simply because the data subject was told of what the policy then was when being convicted or reprimanded. Furthermore, the deletion of this reprimand leading (as it would have to) to deletion of many others would be likely to prejudice the prevention and detection of crime and the apprehension or prosecution of offenders. The court and the CPS need the full information, never mind the fact the police are of the view that for their operational purposes they need the same."

96. Finally, on the argument raised by the individuals that retention of the data violated Article 8 of the Convention, Waller LJ indicated that he was not persuaded that Article 8 § 1 was engaged at all in relation to the retention of the record of a conviction. He was of the view that disclosure might be another matter, but reiterated that the appeal before him was not about disclosure. Even if his conclusion were wrong, he considered that the processing was in accordance with the law and necessary in a democratic society.

97. On the Article 8 question, Lord Justice Carnwath noted as follows:

> "78. ... [W]ith regard to the Human Rights Convention, it is significant that the [Data Protection] Directive is itself specifically linked to the need to respect 'fundamental rights and freedoms, notably the right to privacy...', and that it refers in that respect to the European Convention on Human Rights (Preamble (2), (10)). This suggests that the maintenance of such a complete register of convictions, as implicitly endorsed by Article 8(5) of the Directive, should not normally raise any separate issues under the Convention."

98. He referred to "considerable doubt" as to whether recording the mere fact of a conviction could ever engage Article 8 in any case, distinguishing *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, ECHR, on the basis that it concerned the data of unconvicted persons and was, in his view, accordingly no authority for the proposition that a record of the mere fact of a conviction engaged Article 8.

99. As regards the specific facts of S.P.'s case, given the assurance that she had received from the police that the reprimand would be removed when she reached the age of 18 and the manner in which the police had sought to justify their subsequent decision not to do so, Carnwath LJ considered that the decision of the first-instance tribunal that the retention of the data was unfair and in breach of the first data protection principle could not be faulted in law.

100. Permission to appeal was refused by the Supreme Court on 24 February 2010.

6. R (L) v Commissioner of Police of the Metropolis [2009] UKSC 3

101. In its judgment in *R (L)*, handed down on 29 October 2009, ten days after the Court of Appeal's ruling in *Chief Constable of Humberside*, the Supreme Court considered the Court of Appeal's ruling in *R (X)* (see paragraphs 77-81 above) in the context of a case concerning disclosure of police information under the predecessor of section 113B(4) in the context of an ECRC. The appellant had secured a job as a playground assistant and the school required an ECRC to which the appellant consented. The ECRC disclosed that the appellant had been suspected of child neglect and non-cooperation with social services. The appellant had not been charged with, or convicted of, any offence, nor had she received a caution. Her employment was subsequently terminated and she brought judicial review proceedings, arguing that the disclosure of the information had violated her rights under Article 8. At issue was whether the requirement in the 1997 Act that chief officers provide information which "might be relevant" and "ought to be disclosed" when an ECRC was requested, was proportionate.

102. As to whether Article 8 was engaged by the mere retention of data, after reviewing the case-law of this Court, Lord Hope indicated (at paragraph 27):

> "This line of authority from Strasbourg shows that information about an applicant's convictions which is collected and stored in central records can fall within the scope of private life within the meaning of article 8(1), with the result that it will interfere with the applicant's private life when it is released. It is, in one sense, public information because the convictions took place in public. But the systematic storing of this information in central records means that it is available for disclosure under Part V of the 1997 Act long after the event when everyone other than the person concerned is likely to have forgotten about it. As it recedes into the past, it becomes a part of the person's private life which must be respected. Moreover, much of the other information that may find its way into an ECRC relates to things that happen behind closed doors. A caution takes place in private, and the police gather and record information from a variety of sources which would not otherwise be made public. It may include allegations of criminal behaviour for which there was insufficient evidence to prosecute ... It may even disclose something that could not be described as criminal behaviour at all. The information that was disclosed on the appellant's ECRC was of that kind."

103. He therefore considered that decisions taken by chief constables in the context of ECRCs were likely to fall within the scope of Article 8 in every case as the information in question was stored in files held by the police. He noted that the approach taken by the police to questions of disclosure at the time was modelled on Lord Woolf CJ's ruling in *R (X)* (see paragraphs 77-81 above).

104. Lord Hope indicated that the approach to disclosure under the applicable legislation involved a two-part test. In the first instance, the chief

constable was required to consider whether the information might be relevant. Having concluded in the affirmative, he then had to turn his mind to the question whether the information ought to be included in the certificate. This required consideration of whether there was likely to be an interference with the individual's private life and, if so, whether the interference could be justified. This raised the question whether the Court of Appeal in *R (X)* had struck the balance between the competing interests in the right place.

105. Turning to examine the approach of the Court of Appeal in that case, Lord Hope first endorsed the views expressed there as to the compatibility of the legislation itself with Article 8 (see paragraph 77 above). He noted that, as in that case, the appellant in the present case did not argue that the legislation itself contravened Article 8 and accepted that it could be interpreted and applied in a manner that was proportionate. Lord Hope continued:

> "42. So the issue is essentially one of proportionality. On the one hand there is a pressing social need that children and vulnerable adults should be protected against the risk of harm. On the other there is the applicant's right to respect for her private life. It is of the greatest importance that the balance between these two considerations is struck in the right place ... [T]he use that is being made of the requirement to obtain an ECRC has increased substantially since the scheme was first devised. The number of disclosures of information by means of ECRCs has exceeded 200,000 for each of the last two years (215,640 for 2007/2008; 274,877 for 2008/2009). Not far short of ten per cent of these disclosures have had section 115(7) [now section 113B(4) – see paragraphs 55 above] information on them (17,560 for 2007/2008; 21,045 for 2008/2009). Increasing use of this procedure, and the effects of the release of sensitive information of this kind on the applicants' opportunities for employment or engaging in unpaid work in the community and their ability to establish and develop relations with others, is a cause of very real public concern ..."

106. He noted in this regard that it was no answer to these concerns that the ECRC was issued on the application of the persons concerned. While he accepted that they could choose not to apply for a position of the kind that required a certificate, he considered that they had, in reality, no free choice in the matter if an employer in their chosen profession insisted, as he was entitled to, on an ECRC. He observed:

> "43. ... The answer to the question whether there was any relevant information is likely to determine the outcome of their job application. If relevant information is disclosed they may as a result be cut off from work for which they have considerable training and experience. In some cases they could be excluded permanently from the only work which is likely to be available to them. They consent to the application, but only on the basis that their right to private life is respected."

107. Lord Hope considered that the effect of the approach taken to the issue in *R (X)* had been to tilt the balance against the applicant too far. The correct approach, he explained, was that neither consideration had precedence over the other. He proposed that the relevant guidance to

officers making a decision on disclosure under the provisions should be amended:

> "45. ...so that the precedence that is given to the risk that failure to disclose would cause to the vulnerable group is removed. It should indicate that careful consideration is required in all cases where the disruption to the private life of anyone is judged to be as great, or more so, as the risk of non-disclosure to the vulnerable group. The advice that, where careful consideration is required, the rationale for disclosure should make it very clear why the human rights infringement outweighs the risk posed to the vulnerable group also needs to be reworded. It should no longer be assumed that the presumption was for disclosure unless there was a good reason for not doing so."

108. Lord Neuberger, who indicated that his judgment largely echoed that of Lord Hope, was also firmly of the view that Article 8 was engaged in the case, noting:

> "68. ...An enhanced criminal record certificate ... which contains particulars of any convictions (potentially including spent convictions) or cautions ..., or any other information 'which might be relevant' and which 'ought to be included in the certificate' ...will often have a highly significant effect on the applicant. In the light of the wide ambit of section 115 (extending as it does to social workers and teachers, as well as to those 'regularly caring for, training, supervising or being in sole charge of' children), an adverse ECRC ... will often effectively shut off forever all employment opportunities for the applicant in a large number of different fields ..."

109. He further observed:

> "69. ... Even where the ECRC records a conviction (or caution) for a relatively minor, or questionably relevant, offence, a prospective employer may well feel it safer, particularly in the present culture, which, at least in its historical context, can be said to be unusually risk-averse and judgmental, to reject the applicant ..."

110. Lord Neuberger also rejected the argument that Article 8 was not engaged because under the relevant legislation the claimant herself had requested the ECRC, noting:

> "73. ... Where the legislature imposes on a commonplace action or relationship, such as a job application or selection process, a statutory fetter, whose terms would normally engage a person's Convention right, it cannot avoid the engagement of the right by including in the fetter's procedural provisions a term that the person must agree to those terms. Apart from this proposition being right in principle, it seems to me that, if it were otherwise, there would be an easy procedural device which the legislature could invoke in many cases to by-pass Convention rights."

111. He considered the aim of Part V of the 1997 Act, namely to protect vulnerable people, to be unexceptionable and explained how this was achieved by the requirement that relevant information available to the police about an applicant for a post involving responsibility for such vulnerable people be provided to the prospective employer. He continued:

> "75. ... It is then for that employer to decide whether the information is relevant, and, if so, whether it justifies refusing to employ the applicant. As already mentioned, however, it seems to me realistic to assume that, in the majority of cases, it is likely

> that an adverse ECRC ... will represent something close to a killer blow to the hopes of a person who aspires to any post which falls within the scope of the section ..."

112. Turning to consider whether there was an infringement of Article 8 in the case, Lord Neuberger was prepared to proceed on the basis that there was "nothing objectionable" in the requirement that an ECRC had to contain details of convictions and cautions, even though, he noted, it might on occasions be "rather harsh" on the person concerned. However, like Lord Hope, he was of the view that where other information provided by the chief constable was concerned, the decision on whether to include it in an ECRC had to incorporate a proportionality assessment and it might well be necessary to seek the prior views of the person concerned.

113. Lords Saville and Brown agreed with Lord Hope and, in the case of Lord Brown, Lord Neuberger.

114. Lord Scott, in the minority, considered (at paragraph 57) that if the compilation and retention of the information was unexceptionable, and the information was relevant to the appellant's suitability for the employment sought, then it was difficult to see on what basis her attack on the inclusion of the information in the ECRC could succeed. He continued:

> "58. It is at this point, as it seems to me, that it becomes necessary to remember that it was she who applied for the certificate. I do not doubt that the need for the certificate would have been impressed on her by CSE and that she would have realised that unless she agreed to make the application her chances of obtaining the employment position she desired would be reduced. She may or may not have had in mind the full implications of subsection (7) of section 115 and it would probably not have occurred to her that the history of her delinquent 13 year old son and her failure to have controlled his delinquency would be known to the police and might be considered relevant information. But it cannot, in my opinion, possibly be said that the police response showed a lack of respect for her private life. It was she who, in making the application for an ECRC, invited the exercise by the chief police officer of the statutory duty imposed by section 115(7)."

115. Lord Scott accordingly endorsed the approach taken in *R (X)*.

7. R (C) v Chief Constable of Greater Manchester and Secretary of State for the Home Department [2010] EWCA 1601 and [2011] EWCA Civ 175

116. Following *R (L)*, the High Court quashed a decision by the chief constable to disclose details of a sexual allegation made against the claimant in an ECRC on grounds of procedural impropriety, because the claimant's views had not been sought and because the decision to disclose was disproportionate to the level of risk disclosed. The court granted an injunction to prevent future disclosure.

117. On appeal, the Court of Appeal upheld the decision to quash the disclosure on grounds of procedural impropriety but, emphasising that the primary decision-maker was the chief constable who would take a fresh

decision on the basis of the material now before him, allowed the appeal against the injunction.

8. R (F and another) v Secretary of State for the Home Department [2010] UKSC 17

118. In *R (F and another) v Secretary of State for the Home Department*, the respondents were convicted sex offenders subject to notification requirements under section 82 of the Sexual Offences Act 2003 (SOA 2003), whereby all those sentenced to 30 months' imprisonment or more for a sexual offence are registered on the sex offenders register and subject to a lifelong duty to notify police of their living and travelling arrangements, with no right for review. The question in the appeal was whether the absence of any right to review rendered the notification requirements disproportionate to the legitimate aims they sought to pursue and thus incompatible with Article 8 of the Convention. Lord Phillips noted:

> "41. The issue in this case is one of proportionality. It is common ground that the notification requirements interfere with offenders' article 8 rights, that this interference is in accordance with the law and that it is directed at the legitimate aims of the prevention of crime and the protection of the rights and freedoms of others. The issue is whether the notification requirements, as embodied in the 2003 Act, and without any right to a review, are proportionate to that aim. That issue requires consideration of three questions. (i) What is the extent of the interference with article 8 rights? (ii) How valuable are the notification requirements in achieving the legitimate aims? and (iii) To what extent would that value be eroded if the notification requirements were made subject to review? The issue is a narrow one. The respondents' case is that the notification requirements cannot be proportionate in the absence of any right to a review. The challenge has been to the absence of any right to a review, not to some of the features of the notification requirements that have the potential to be particularly onerous."

119. He found that the notification requirements were capable of causing significant interference with Article 8 rights. However, he continued (at paragraph 51):

> "... This case turns, however, on one critical issue. If some of those who are subject to lifetime notification requirements no longer pose any significant risk of committing further sexual offences and it is possible for them to demonstrate that this is the case, there is no point in subjecting them to supervision or management or to the interference with their article 8 rights involved in visits to their local police stations in order to provide information about their places of residence and their travel plans. Indeed subjecting them to these requirements can only impose an unnecessary and unproductive burden on the responsible authorities. We were informed that there are now some 24,000 ex-offenders subject to notification requirements and this number will inevitably grow."

120. He concluded:

> "56. No evidence has been placed before this court or the courts below that demonstrates that it is not possible to identify from among those convicted of serious offences, at any stage in their lives, some at least who pose no significant risk of re-

offending. It is equally true that no evidence has been adduced that demonstrates that this is possible. This may well be because the necessary research has not been carried out to enable firm conclusions to be drawn on this topic. If uncertainty exists can this render proportionate the imposition of notification requirements for life *without review* under the precautionary principle? I do not believe that it can.

57. ... I think that it is obvious that there must be some circumstances in which an appropriate tribunal could reliably conclude that the risk of an individual carrying out a further sexual offence can be discounted to the extent that continuance of notification requirements is unjustified. As the courts below have observed, it is open to the legislature to impose an appropriately high threshold for review. Registration systems for sexual offenders are not uncommon in other jurisdictions. Those acting for the first respondent have drawn attention to registration requirements for sexual offenders in France, Ireland, the seven Australian States, Canada, South Africa and the United States. Almost all of these have provisions for review. This does not suggest that the review exercise is not practicable.

58. For these reasons I have concluded that ... the notification requirements constitute a disproportionate interference with article 8 rights because they make no provision for individual review of the requirements."

121. The Supreme Court issued a declaration that section 82 of the SOA 2003 was incompatible with the Convention.

III. RELEVANT COUNCIL OF EUROPE TEXTS

A. Data protection

122. The Council of Europe Convention of 1981 for the protection of individuals with regard to automatic processing of personal data ("the Data Protection Convention"), which entered into force for the United Kingdom on 1 December 1987, defines "personal data" as any information relating to an identified or identifiable individual ("data subject"). Article 5, which deals with quality of data, provides:

"Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

...

e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

123. Article 6 deals with "special categories of data" and stipulates that personal data relating to criminal convictions may not be processed automatically unless domestic law provides appropriate safeguards.

124. Pursuant to Article 9, derogations are permitted where they are necessary in a democratic society in the interests of, *inter alia*, public safety, the suppression of criminal offences or protecting the rights and freedoms of others.

125. The Committee of Ministers adopted Recommendation No. R (87) 15 regulating the use of personal data in the police sector on 17 September 1987, in the context of a sectoral approach to data protection intended to adapt the principles of the Data Protection Convention to the specific requirements of particular sectors. An Explanatory Memorandum ("EM") sets out the background to the Recommendation's adoption, and notes at paragraph 4:

> "Given the increased activities of police forces in the lives of individuals necessitated by new threats to society posed by terrorism, drug delinquency, etc as well as a general increase in criminality, it was felt even more necessary to establish clear guidelines for the police sector which indicate the necessary balance needed in our societies between the rights of the individual and legitimate police activities when the latter have recourse to data-processing techniques."

126. It further observes that concerns which prompted the elaboration of the Data Protection Convention in regard to the increasing recourse to automation in all sectors are most acutely felt in the police sector, for it is in this domain that the consequences of a violation of the basic principles laid down in the Convention could weigh most heavily on the individual.

127. As regards the derogations permitted under Article 9 of the Data Protection Convention, the EM reiterates that they are only permitted if provided for by law and necessary in a democratic society in the interests of, *inter alia*, the "suppression of criminal offences". It continues:

> "20 ... Bearing in mind that the European Court of Human Rights in its judgment in the Malone Case laid down a number of strict criteria (precision, certainty, foreseeability, etc), it is thought that the principles contained in this non-binding legal instrument can provide helpful guidance to the legislator as to the interpretation of the derogation in Article 9, paragraph 2, of the Data Protection Convention when regulating the collection, use, etc of personal data in the police sector. This point should be borne in mind, for example, in the context of paragraph 2.1."

128. Principle 1.1 of the Recommendation provides:

> "Each member state should have an independent supervisory authority outside the police sector which should be responsible for ensuring respect for the principles contained in this recommendation."

129. The EM emphasises the importance of such supervisory authority enjoying genuine independence from police control.

130. Principle 2 concerns collection of data and includes the following:

"2.1 The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation."

131. The EM explains that Principle 2.1 excludes an "open-ended, indiscriminate" collection of data by the police and expresses a "qualitative and quantitative" approach to Article 5(c) of the Data Protection Convention. The Principle attempts to fix the boundaries to the exception in Article 9 of the Data Protection Convention by limiting the collection of personal data to such as are necessary for the prevention of a real danger or the suppression of a specific criminal offence, unless domestic law clearly authorises wider police powers to gather information.

132. Storage of data is addressed in Principle 3. Principle 3.1 provides that as far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law. The EM explains:

"49. Personal data when collected will subsequently be the subject of a decision concerning their storage in police files. *Principle 3.1* addresses the requirements of accuracy and storage limitation. The data stored should be accurate and limited to such data as are necessary to enable the police to perform its lawful tasks ...

50. This principle is important given the fact that the commitment of personal data to a police file may lead to a permanent record and indiscriminate storage of data may prejudice the rights and freedoms of the individual. It is also in the interests of the police that it has only accurate and reliable data at its disposal."

133. Principle 5 deals with communication of data. Principle 5.1 permits communication of data between police bodies, to be used for police purposes, if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies. In respect of communication to other public bodies, Principle 5.2 stipulates:

"5.2.i. Communication of data to other public bodies should only be permissible if, in a particular case:

a. there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority, or if

b. these data are indispensable to the recipient to enable him to fulfil his own lawful task and provided that the aim of the collection or processing to be carried out by the recipient is not incompatible with the original processing, and the legal obligations of the communicating body are not contrary to this.

5.2.ii. Furthermore, communication to other public bodies is exceptionally permissible if, in a particular case:

...

b. the communication is necessary so as to prevent a serious and imminent danger."

134. As to the possibility of communicating indispensable data to public bodies under Principle 5.2.i.b, the EM explains that it is recognised that certain public bodies engage in activities which are similar in some ways to police activities and that information held by the police may be of value to those activities. Regarding the possibility of communicating data to prevent a serious and imminent danger, the EM recalls that this will only "exceptionally" allow communication and that the danger must be both serious and imminent, given that Principle 5.2.ii is only concerned with exceptional cases justifying communication.

135. As regards communication to private parties, Principle 5.3 provides:

"5.3.ii. The communication of data to private parties should only be permissible if, in a particular case, there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority.

5.3.ii. Communication to private parties is exceptionally permissible if, in a particular case:

...

b. the communication is necessary so as to prevent a serious and imminent danger."

136. The EM acknowledges that it may occasionally be necessary for the police to communicate data to private bodies, although not on the same scale as envisaged in the case of mutual assistance between the police and other public bodies. It continues:

"Once again, *Principle 5.3* treats these as exceptional cases, requiring a clear legal obligation or authorisation (for example the consent of a magistrate), or the consent of the supervisory authority. In the absence of these factors, Principle 5.3 repeats the same conditions set out in Principle 5.2.ii."

137. Concerning Principle 5 generally, the EM notes:

"Outside the framework of communication within the police sector, the conditions governing transfer are stricter, given the fact that the communication may be for non-police purposes *stricto sensu.* The exceptional nature of the circumstances allowing communication set out in *Principles 5.2 and 5.3* is stressed. It will be noted that circumstances *a* and *b* in both *Principles 5.2.ii and 5.3.ii* are specifically referred to as 'exceptional'."

138. Principle 7 deals with length of storage and updating of data. Pursuant to Principle 7.1 measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored. It further provides:

"... For this purpose, consideration shall in particular be given to the following criteria: the need to retain data in the light of the conclusion of an inquiry into a particular case; a final judicial decision, in particular an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject, particular categories of data."

139. The EM explains that it is essential that periodic reviews of police files are undertaken to ensure that they are purged of superfluous or inaccurate data and kept up to date. It notes that Principle 7.1 lists certain considerations which should be borne in mind when determining whether or not data continue to be necessary for the prevention and suppression of crime or for the maintenance of public order.

140. Principle 7.2 provides:

> "Rules aimed at fixing storage periods for the different categories of personal data as well as regular checks on their quality should be established in agreement with the supervisory authority or in accordance with domestic law."

141. The EM notes that domestic law may authorise the means for laying down such rules or that, alternatively, rules could be formulated by the supervisory authority itself in consultation with police bodies. It explains that where the police themselves elaborate rules, the supervisory authority should be consulted as to their content and application.

B. Rehabilitation of offenders

142. Recommendation No. R (84) 10 of the Committee of Ministers on the criminal record and rehabilitation of convicted persons (adopted on 21 June 1984) notes in its preamble that any use of criminal record data outside the criminal trial context may jeopardise the convicted person's chances of social reintegration and should therefore be restricted "to the utmost". It invited member States to review their legislation with a view to introducing a number of measures where necessary, including provisions limiting the communication of criminal record information and provisions on rehabilitation of offenders, which would imply the prohibition of any reference to the convictions of a rehabilitated person except on compelling grounds provided for in national law.

IV. RELEVANT EUROPEAN UNION TEXTS

A. The Treaty on the Functioning of the European Union ("TFEU")

143. The TFEU sets out in Article 16 the right to the protection of personal data concerning them. It requires the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law; and the rules relating to the free movement of such data.

B. Charter of Fundamental Rights of the European Union (2000)

144. The EU Charter of Fundamental Rights includes the right to protection of personal data. Article 8 of the Charter reads:

> "1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority."

C. Other instruments

145. 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 ("the Data Protection Directive") provides that the object of national laws on the processing of personal data is notably to protect the right to privacy as recognised both in Article 8 of the European Convention on Human Rights and in the general principles of Community law. The Directive sets out a number of principles in order to give substance to and amplify those contained in the Data Protection Convention of the Council of Europe. It allows Member States to adopt legislative measures to restrict the scope of certain obligations and rights provided for in the Directive when such a restriction constitutes notably a necessary measure for the prevention, investigation, detection and prosecution of criminal offences (Article 13).

146. Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters ("the Data Protection Framework Decision") was adopted on 27 November 2008. Its purpose is to ensure a high level of protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data in the framework of cross-border police and judicial cooperation in criminal matters while guaranteeing a high level of public safety.

147. Article 3 of the Data Protection Framework Decision provides that personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes and may be processed only for the same purpose for which data were collected. Processing of the data must be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected. Article 5 provides that appropriate time-limits must be established for the erasure of personal data or for a

periodic review of the need for the storage of the data. Procedural measures must be in place to ensure that these time-limits are observed.

148. In January 2012 the European Commission published proposals, based *inter alia* on Article 16 TFEU, for the comprehensive reform of the EU's data protection framework. The proposals are currently under negotiation.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

149. The applicant complained under Article 7 about the retention and disclosure of her caution data, referring in particular to the change in policy subsequent to the administration of the caution, which has led to her caution being retained for life, and the impact on her employment prospects.

150. The Court reiterates that it is master of the characterisation to be given in law to the facts of the case (see *Guerra and Others v. Italy*, judgment of 19 February 1998, *Reports of Judgments and Decisions* 1998-I, p. 223, § 44; *Tătar and Tătar v. Romania* (dec.), no. 67021/01, § 47, 5 July 2007; and *Scoppola v. Italy (no. 2)* [GC], no. 10249/03, § 54, 17 September 2009). By virtue of the *jura novit curia* principle, it has, for example, previously considered of its own motion complaints under Articles not relied on by the parties (see, for example, *Scoppola (No. 2)*, cited above, §§ 54-55; *B.B. v. France*, no. 5335/06, § 56, 17 December 2009 and *Şerife Yiğit v. Turkey* [GC], no. 3976/05, §§ 52-53, 2 November 2010). The Court considers that in the light of its case-law (see, for example, *Leander v. Sweden*, 26 March 1987, Series A no. 116; *S. and Marper*, cited above; and *B.B.*, cited above) it is appropriate to examine the applicant's complaints first from the standpoint of Article 8 of the Convention, which provides:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

151. The Government contended that no issue under Article 8 arose.

A. Admissibility

1. The parties' submissions

(a) The Government

152. The Government invited the Court to declare the application inadmissible pursuant to Article 35 §§ 1 and 4 of the Convention for failure to exhaust domestic remedies, emphasising the importance of allowing the State the opportunity to prevent or put right the alleged violations.

153. They noted that the applicant had not attempted to bring any legal proceedings to challenge the police retention of the caution or its inclusion on the criminal record certificate. Her reference to an application for legal aid was in respect of a potential claim against the Trust for failing to employ her, not a challenge to the retention or disclosure of the caution data. The advice from her lawyer in 2006 related to whether the issue of the caution itself could be revisited and not the legality of its retention beyond the five-year period.

154. The Government emphasised that as a matter of both principle and precedent, judicial review was available for an aggrieved individual to challenge police retention of the data in question. They contended that in light of the Human Rights Act (see paragraphs 72-76 above), the applicant could have pursued any allegation of a violation of a Convention right. She could have made a similar complaint to the Information Commissioner under the Data Protection Act (see paragraph 71 above). Neither of these remedies had been pursued. As a consequence of her failure, the domestic courts had not been able to examine her complaints and to take action if they agreed that a violation had occurred. The Government referred to the judicial review cases listed above concerning ECRCs as well as the Court of Appeal's consideration in *Chief Constable of Humberside* of the retention of police information as evidence that the courts in England adopted a careful and considered analysis of the competing rights. In particular, the recent case of *R (L)* was evidence that the courts were willing to give careful scrutiny to the lawfulness and proportionality of retention and disclosure of information under the 1997 Act by reference to Convention rights. The same general principles would be expected to be applied by the Northern Irish courts.

155. Then Government further explained that in any judicial review proceedings, the defendant, who would be the relevant chief constable, would be entitled to adduce evidence to explain why a particular retention decision was made, and what ameliorating measures might be operated.

(b) The applicant

156. The applicant emphasised that the burden of proof was on a Government claiming non-exhaustion to satisfy the Court that an effective remedy was available in theory and in practice at the relevant time. Further, she noted that the rule of exhaustion was neither absolute nor capable of being applied automatically: it had to be applied with some degree of flexibility and without excessive formalism in the human rights context.

157. The applicant also disputed the suggestion that a remedy was provided by the Data Protection Act. She noted the possibility for an individual to check the accuracy of data held about them and to seek amendment of inaccurate data, but emphasised that she did not dispute the accuracy of the data in her case.

158. She explained that she had sought legal advice on the merits of judicial review and had applied for legal aid, which had been refused. In her view this had determined her attempt to exhaust domestic remedies.

2. The Court's assessment

159. The Court observes that the applicant's complaint to the Court was lodged following the withdrawal of an offer of employment which had been made to her after she had disclosed, and the Criminal Records Office had verified, the existence of a caution. The Court is satisfied that the job offer was withdrawn on account of the disclosure of the caution; the Government have not sought to argue otherwise. The applicant complained about the change in policy regarding retention of caution data, which means that it would now be retained for life, and the impact of this change on her employment prospects. It is clear that for as long as her data are retained and capable of being disclosed, she remains a victim of any potential violation of Article 8 arising from retention or disclosure. As Waller LJ noted in *Chief Constable of Humberside*, the complaint about retention in reality flows not from the retention itself but from the fact that, if retained, disclosure may follow (see paragraph 94 above). It is clear that if the applicant was able to have her data deleted, then it would no longer be available for disclosure. Alternatively, a remedy which prevented the disclosure of the data might have provided adequate redress. The Court's examination of whether she has exhausted available remedies must therefore necessarily encompass alleged past, present and potential future violations in respect of the retention and disclosure of the applicant's data.

160. In this regard the Court observes that the framework governing retention and disclosure of criminal record data in Northern Ireland has undergone a number of changes, both legislative and policy-based, since the administration of the applicant's caution in 2000. As the applicant's complaint is of a continuing nature, the Court must consider the Government's objection in the context of the different applicable regimes.

161. It is appropriate to address first the applicant's contention that she sought legal advice and legal aid with a view to challenging the retention and disclosure of her caution data. In this regard, the Court notes, as the Government pointed out, that the legal advice she received from her solicitors in 2006 concerned the prospects of a challenge to the issue of the caution, and not its retention or disclosure (see paragraph 15 above). Similarly, as the Government explained, the applicant's attempt to secure legal aid in 2007 was in respect of a potential claim against the Trust for refusing to employ her, and not against the chief constable for retention and disclosure of her caution data (see paragraph 17 above). The Court therefore accepts that she has not sought to pursue legal proceedings against the police in respect of the retention or disclosure of her data.

162. Article 35 § 1 requires that the applicant exhaust available and effective domestic remedies before seeking redress before this Court. The Court recalls that where the Government claim non-exhaustion they must satisfy the Court that the remedy proposed was an effective one available in theory and in practice at the relevant time, that is to say, that it was accessible, was capable of providing redress in respect of the applicant's complaints and offered reasonable prospects of success (see, *inter alia*, *Akdivar and Others v. Turkey*, 16 September 1996, § 68, *Reports of Judgments and Decisions* 1996-IV; *Sejdovic v. Italy* [GC], no. 56581/00, § 46, ECHR 2006-II; and *Kennedy v. the United Kingdom*, no. 26839/05, § 109, 18 May 2010).

163. The application of the rule of exhaustion of domestic remedies must make due allowance for the fact that it is being applied in the context of machinery for the protection of human rights that the Contracting States have agreed to set up. The Court has accordingly recognised that Article 35 § 1 must be applied with some degree of flexibility and without excessive formalism. It has further recognised that the rule of exhaustion is neither absolute nor capable of being applied automatically; for the purposes of reviewing whether it has been observed, it is essential to have regard to the circumstances of the individual case. This means, in particular, that the Court must take realistic account not only of the existence of formal remedies in the legal system of the Contracting State concerned but also of the general context in which they operate, as well as the personal circumstances of the applicant. It must then examine whether, in all the circumstances of the case, the applicant did everything that could reasonably be expected of him or her to exhaust domestic remedies (see *İlhan v. Turkey* [GC], no. 22277/93, § 59, ECHR 2000-VII; *D.H. and Others v. the Czech Republic* [GC], no. 57325/00, § 116, ECHR 2007-IV; and *Demopoulos and Others v. Turkey* (dec.) [GC], nos. 46113/99, 3843/02, 13751/02, 13466/03, 10200/04, 14163/04, 19993/04 and 21819/04, § 70, ECHR 2010).

164. The Government argued that the applicant could have brought legal proceedings to challenge the police retention of the caution or its inclusion in any criminal record certificate. Such an action could have proceeded by way of judicial review or by way of a complaint to the Information Commissioner under the Data Protection Act. In support of their submissions, the Government have referred to a number of cases decided by the domestic courts as illustrative of the courts' jurisdiction and willingness to assess compliance of retention or disclosure of criminal record data with Article 8 of the Convention (see paragraphs 77-121 above).

165. The Court observes, first, that the majority of these cases concerned only disclosure, and not retention, of criminal record data. Second, the disclosure in the cases related to other "information" pursuant to section 113B(4) (or its predecessor section) of the 1997 Act (see paragraph 55 above), and not disclosure of caution or conviction information either under common law police powers or pursuant to section 113A(3) or section 113B(3) of the Act (see paragraphs 49 and 54 above). Third, none of the cases to which the Government have referred were brought in respect of the legal framework in place in Northern Ireland. It is with these considerations in mind that the Court now turns to examine, in the circumstances of the applicant's case and in light of the judgments identified, whether either of the remedies proposed by the Government was an effective one available in theory and in practice, that is to say, that it was accessible, was capable of providing redress in respect of the applicant's complaints and offered reasonable prospects of success.

166. The Court notes that in 2006 retention and disclosure of caution data in Northern Ireland were carried out on the basis of the common law powers of the police (see paragraphs 24 and 47 above), and that the general principles of the Data Protection Act applied to the processing of any data. Guidance was available in the form of the MOPI Guidance (see paragraph 36-41 and 58-59 above) and the ACPO Guidelines (see paragraphs 42-46 and 60 above); it is not clear whether the 2005 Code of Practice was adopted by the PSNI (see paragraphs 33-35 above).

167. The guidance demonstrates that in deciding whether to retain data, the police enjoy a certain degree of discretion (see paragraphs 37, 39-41 and 46 above). However, the MOPI Guidance refers to a "presumption" in favour of retention where the data are considered necessary and recommends that in cases concerning serious offences, records be retained until the subject has reached one hundred years of age (see paragraphs 39-40 above). The ACPO Guidelines specify in their general principles that records are to be retained until a subject reaches one hundred years of age; it appears that no distinction is drawn between offences for the purpose of the length of the retention period (see paragraph 45 above). Although the Guidelines refer to the discretion enjoyed by chief constables in "exceptional circumstances" to authorise deletion of data, the circumstances

envisaged are very limited: Appendix 2 indicates that exceptional cases will be rare and gives the example of where it is established beyond reasonable doubt that no offence existed (see paragraph 46 above).

168. As regards disclosure of criminal record information for employment purposes, the MOPI Guidance refers to the statutory scheme for disclosure created by the 1997 Act and to the need for a balancing exercise to be conducted in the context of the common law powers of the police to disclose data (see paragraphs 58-59 above). The ACPO Guidelines set out the "stepping down" policy of limiting access to certain data after a certain time period has elapsed; however, it appears that the "stepping down" policy does not apply to cases concerning requests for criminal record checks (see paragraphs 60 and 89 above).

169. In these circumstances, and having regard in particular to the provisions of the Human Rights Act (see paragraphs 72-76 above) and the Data Protection Act (see paragraphs 65-71 above), the Court is satisfied that the applicant could in theory have sought to commence judicial review proceedings in respect of a decision to retain or disclose her caution data or could have made a complaint to the Information Commissioner, seeking to have the caution data deleted or to prevent its disclosure. In any such proceedings she could have sought to rely on the data protection principles and Article 8 of the Convention. It is therefore necessary to examine whether such proceedings offered reasonable prospects of success.

170. First, as regards retention of criminal record data, no judgment handed down by late 2006 or early 2007 in which individuals sought to challenge retention of criminal record data, and in particular data relating to a caution, relying on the Convention or on the data protection principles has been brought to the attention of the Court. Given the nature of the guidance on retention to which the Court has referred above (see paragraph 167 above) and the generous approach to the powers of the police to retain data set out therein, this is not surprising. The potential for a successful challenge to the exercise of the chief constable's discretion to retain data, or indeed to the policy itself, was further diminished by the position of the domestic courts at the time, which tended to consider that Article 8 did not apply to mere retention of data or, if it did, that any interference was minor (see the House of Lords' judgment regarding retention of DNA data which was challenged in *S. and Marper*, cited above, summarised at §§ 15-25 of that judgment).

171. As regards a challenge to the disclosure of the caution data, the Court observes that in its 2004 judgment in *R (X)* dealing with disclosure under the 1997 Act of other "information" on an ECRC under the 1997 Act, the Court of Appeal took a robust approach to the exercise of discretion by the chief constable in choosing to disclose information in the context of a criminal record check. Lord Woolf CJ indicated that the chief constable was "under a duty" to disclose any information which might be relevant unless

there was some good reason for not making the disclosure (see paragraph 79 above). He further found that the chief constable was not required to invite representations from the subject of the criminal record check before deciding what to include in the certificate (see paragraph 80 above). Specifically on the question of Article 8 considerations, the Court of Appeal expressed the view that it was difficult to see how a chief constable's decision to disclose could ever be challenged (see paragraph 81 above). The Court observes that the case was decided against the backdrop of a clearly-defined legislative framework (i.e., the 1997 Act, which was in force in England and Wales at the time) which the court took to be in compliance with Article 8 (see paragraph 78 above). However, it considers that the court's approach to the exercise of discretion is nonetheless indicative of a wide discretion afforded to the police to decide on questions of disclosure and a rejection of any need for the participation of the data subject in the decision to disclose criminal record data. It is also relevant to emphasise that the applicant's case did not concern disclosure of other information under section 113B(4) but of caution data, the mandatory disclosure of which required by the 1997 Act reveals the view of the legislature that such information will always be relevant. It is significant that the Government have not pointed to any case decided at that time in which an individual had successfully challenged a decision to disclose criminal record data, either concerning convictions and caution data or in respect of section 113B(4) information. Further, no details of any specific guidance setting out the factors which had to be taken into account in making any disclosure decision in the employment context in Northern Ireland at the time have been provided to the Court.

172. Having regard to the continuing nature of the applicant's complaint about the retention and potential future disclosure of her data (see paragraph 159 above), it is also relevant to examine developments which have occurred since the applicant's case was lodged.

173. First, as regards retention of criminal record data, in 2009 the Court of Appeal handed down its judgment in the case of *Chief Constable of Humberside*, which considered whether the Data Protection Act or Article 8 required deletion of old convictions following a decision by the Information Commissioner that it did. While the case was brought by a number of individuals seeking to have their own data deleted, Waller LJ emphasised that the ramifications of the cases were far wider than the cases themselves, since if the convictions at issue were to be deleted and the police were to treat people consistently, the result would be the deletion of around one million convictions (see paragraph 88 above). It follows that the scope of the appeals went beyond the personal interests of the individuals directly involved in the proceedings so that, in that sense, the decision of the Court of Appeal was of more general application and affected others, such as the applicant, in a similar position.

174. Waller LJ considered the argument that there was no statutory obligation on the police to retain data under the Police Act, but noted that "on any view" the Act seemed to recognise that the data would be there to be provided (see paragraph 90 above). He was of the opinion that in assessing whether the data retained were excessive or were being retained for longer than necessary, there was "only one answer" since in order to be able to supply accurate records of convictions, a complete record of conviction, spent or otherwise, was required. This was, he said, a "complete answer to the appeal" (see paragraph 92 above). Even if a narrower approach to police purposes were to be adopted, Waller LJ indicated that the retention of the data would remain lawful because if the police said rationally and reasonably that convictions, however old or minor, had a value in the work they did, then that should be the end of the matter (see paragraph 93 above). As to whether the retention of data violated Article 8 of the Convention, Waller LJ doubted whether Article 8 applied but, even if it did, considered that the retention was in accordance with the law and necessary in a democratic society (see paragraph 96 above). Carnwath LJ also expressed some doubt as to whether Article 8 applied to the recording of a conviction (see paragraph 98 above).

175. It is also of relevance that one of the individuals in that case sought to argue that continued retention of data relating to a reprimand was unfair because she had been assured that it would be removed when she reached the age of eighteen. Waller LJ, with whom Hughes LJ agreed, dismissed this argument, indicating that if it was fair to retain data under the new policy then it did not become unfair simply because the individual had been told what the policy was at the time she was reprimanded. He further referred to the fact that the deletion of her reprimand would lead to the deletion of many others and would therefore be likely to prejudice the prevention and detection of crime and the apprehension and prosecution of offenders (see paragraph 95 above).

176. Following the Court of Appeal's findings in *Chief Constable of Humberside*, and the refusal of leave by the Supreme Court (see paragraph 100 above), it is not clear how any proceedings commenced or complaint lodged by the applicant in order to challenge the retention of her caution data could seek to distinguish that case and thus offer her reasonable prospects of success in obtaining deletion of her data. The Government have not specified how she could have done so, nor have they clarified whether, in their view, in the light of that judgment, the judicial review remedy proposed by them offered to the applicant "reasonable prospects of success" in respect of the continued retention of her data.

177. Second, as regards the disclosure of the applicant's data, the position changed significantly with the entry into force in Northern Ireland of the relevant provisions of the Police Act 1997. While the applicant does not allege that her data have been disclosed pursuant to these provisions, as

the Court has noted above her complaint clearly encompasses the continuing threat of disclosure arising from the fact that her data have been retained (see paragraph 159 above). Sections 113A(3) and 113B(3) impose a mandatory obligation to disclose data pertaining to cautions held in central records, including cautions which are spent pursuant to legislation covering rehabilitation of offenders, in both CRCs and ECRCs (see paragraphs 49 and 54 above). Unlike the case of other information included in an ECRC pursuant to section 113B(4) (see paragraph 55 above), there is no discretion afforded to chief constables to choose to omit data pertaining to cautions, and any such data retained in central records must accordingly be disclosed.

178. In these circumstances, the Court is satisfied that a challenge to the disclosure of caution data following the entry into force of the 1997 Act in Northern Ireland would necessarily have to proceed by way of a challenge to sections 113A and 113B themselves. Pursuant to the Human Rights Act, it would be open to the applicant to request that the provisions be interpreted in a manner compatible with the Convention or to seek a declaration of incompatibility pursuant to section 4(2) of Act (see paragraphs 72-73 above). The Government did not comment on whether, in their view, the relevant provisions could be interpreted in a compatible manner. In light of the information before it, and in particular given the clear terms of the legislation, the Court is not persuaded that the possibility of proceedings seeking a compliant interpretation under the Human Rights Act offered reasonable prospects of success. Although a declaration of incompatibility could be sought, there is no obligation following the making of such a declaration for the Government to amend the legislation and no entitlement to damages arises. The Court has therefore previously indicated that a declaration of incompatibility cannot be considered an effective remedy for the purposes of Article 35 § 1 of the Convention (see *Burden v. the United Kingdom* [GC], no. 13378/05, §§ 43-44, ECHR 2008; and *Kennedy*, cited above, § 109) and it sees no reason to reach a different conclusion in the present case.

179. Having regard to its review of the case-law above, to the failure of the Government to point to any case where a claim for judicial review of a decision to retain data or a complaint under the Data Protection Act regarding retention was successful, and to the provisions of sections 113A and 113B of the Police Act, the Court is not satisfied that the Government have demonstrated the existence of a remedy apt to afford the applicant redress for her complaints or offering reasonable prospects of success either in 2007, when she lodged her case with this Court, or at the present time. The Government's objection is accordingly dismissed.

180. The Court further notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention and is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

(a) The applicant

181. The applicant argued that retention of the caution data engaged her right to respect for her private life because it had affected her ability to secure employment in her chosen field.

182. Although she accepted that she had disclosed the caution herself, she had done so because she was obliged to and she considered that it was simply not arguable that she could have simply concealed the fact of the caution.

183. She contended that it was necessary to examine the proportionality of the retention of the caution data on the criminal record for a prolonged period. For this purpose, individual circumstances had to be considered. While the applicant accepted that the change in policy was intended to secure the protection of children, the automatic nature of the rule was problematic. In the applicant's case, the caution related to action taken in the heat of the moment in a family situation with very specific circumstances. There was no suggestion that the applicant represented a general threat to children and the continued retention of her data therefore did not, she contended, pursue the legitimate aim of protecting children. It was clear from the correspondence with the police that the only relevant factor was the code applied to her caution (see paragraph 14 above). She further argued that there was no review process to assess the necessity of continued retention of the caution data.

(b) The Government

184. The Government submitted that there was a distinction between the mere retention of data and their subsequent disclosure. They contended that mere retention had no particular effect on an individual or his rights under Article 8, referring to Waller LJ's comments in *Chief Constable of Humberside* (see paragraph 97 above). They distinguished the Court's judgment in *S. and Marper* on the grounds that the retention of the caution data in the present case did not concern any latent information about an individual of the type that might exist in cellular samples. In their view, retention of criminal record data by the police was an inevitable and commonplace feature of any effective and proper criminal justice system and did not interfere with Article 8 rights in any meaningful way.

185. In any event the Government argued that both retention and disclosure of the caution data complied with Article 8 § 2 of the Convention. As regards retention, the Government emphasised that it occurred in accordance with the law in a number of well-established ways,

pursuant to common law powers as police officers and their statutory powers of policing and in accordance with the principles set out in the Data Protection Act. It pursued the legitimate aims of public safety, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. Finally, retention was also necessary and proportionate. Retention was primarily a matter of judgment for the individual police force or Government in question in accordance with the margin of appreciation. However, retention was usually necessary and proportionate as it was important for the police to retain records of what had happened. They referred in this respect to the MOPI Guidance 2006 (see paragraphs 36-41 above).

186. In respect of disclosure, the Government emphasised that in the applicant's case it took place at her request and with her consent. However, and in any case, they argued that an assessment of the need for disclosure was a matter for the policy judgment of the State in question and fell within the margin of appreciation, regard being had to the objectives of the legislation and the relevance of the information to the employment being sought. An individual dissatisfied with disclosure in her case could challenge it by way of judicial review or pursue a complaint to the Information Commissioner. In the applicant's case, the disclosure was made in accordance with the law and the applicant does not suggest otherwise. It took place for a legitimate purpose, namely the prevention of disorder and crime and the protection of the rights and freedoms of others. Finally it was both necessary and proportionate to the aim pursued. In this regard it was relevant that the applicant herself requested the disclosure; she was applying for a job working with children and vulnerable adults; she recognised the relevance of the incident to her employment; and the disclosure was factually correct.

2. The Court's assessment

(a) Applicability of Article 8

187. The Court reiterates that both the storing of information relating to an individual's private life and the release of such information come within the scope of Article 8 § 1 (see *Leander*, cited above, § 48; *Amann v. Switzerland* [GC], no. 27798/95, §§ 65 and 69-70, ECHR 2000-II; *Rotaru v. Romania* [GC], no. 28341/95, § 43, ECHR 2000-V. See also *S. and Marper*, cited above, § 67; and *Khelili v. Switzerland*, no. 16188/07, § 55, 18 October 2011, on the applicability of Article 8 to the storage of data). Even public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities (see *Rotaru*, cited above, § 43; *P.G. and J.H.*, cited above, § 57; *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 72, ECHR 2006-VII; and *Cemalettin Canlı v. Turkey*, no. 22427/04, § 33, 18 November 2008). This is

all the more true where the information concerns a person's distant past (*Rotaru*, cited above, § 43; and *Cemalettin Canlı*, cited above, § 33). The question therefore arises in the present case whether the data relating to the applicant's caution stored in police records constitute data relating to the applicant's "private life" and, if so, whether there has been an interference with her right to respect for private life.

188. The Court notes at the outset that the data in question constitute both "personal data" and "sensitive personal data" within the meaning of the Data Protection Act 1998 (see paragraph 67 above). They also constitute "personal data" and are identified as a special category of data under the Council of Europe's Data Protection Convention (see paragraphs 122-123 above). Further, the data form part of the applicant's criminal record (see *Rotaru*, cited above, §§ 43-46; and *B.B.*, cited above, § 57). In this regard the Court, like Lord Hope in *R (L)*, emphasises that although data contained in the criminal record are, in one sense, public information, their systematic storing in central records means that they are available for disclosure long after the event when everyone other than the person concerned is likely to have forgotten about it, and all the more so where, as in the present case, the caution has occurred in private. Thus as the conviction or caution itself recedes into the past, it becomes a part of the person's private life which must be respected (see *Rotaru*, cited above, §§ 43-44). In the present case, the administration of the caution occurred almost twelve years ago.

189. The Government referred several times in their written submissions to the fact that the applicant herself disclosed details of the caution to her prospective employer, and that the details she disclosed were merely confirmed by the Criminal Records Office. The Court observes that the posts for which the applicant applied were subject to vetting. In this context she was asked for details of her conviction and caution history and provided them as requested. The Court notes and agrees with the comments of Lords Hope and Neuberger in *R (L)*, to the effect that the fact that disclosure follows upon a request by the data subject or with her consent is no answer to concerns regarding the compatibility of disclosure with Article 8 of the Convention. Individuals have no real choice if an employer in their chosen profession insists, and is entitled to do so, on disclosure: as Lord Hope noted, consent to a request for criminal record data is conditional on the right to respect for private life being respected (see paragraph 106 above). The applicant's agreement to disclosure does not deprive her of the protection afforded by the Convention (see paragraph 110 above).

190. The Court therefore finds that Article 8 applies in the present case to the retention and disclosure of the caution, and that the retention and disclosure of the data amount to an interference with that Article.

(b) Compliance with Article 8

191. In order to be justified under Article 8 § 2 of the Convention, any interference must be in accordance with the law, pursue one of the listed legitimate aims and be necessary in a democratic society.

192. The applicant did not make any submissions as to whether the interference was lawful. The Government contended that the interference was in accordance with the law.

193. The requirement that any interference must be "in accordance with the law" under Article 8 § 2 means that the impugned measure must have some basis in domestic law and be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise (see *Malone v. the United Kingdom*, 2 August 1984, §§ 66-68, Series A no. 82; *Rotaru*, cited above, §§ 52 and 55; *Liberty and Others v. the United Kingdom*, no. 58243/00, § 59, 1 July 2008; and *S. and Marper*, cited above, § 95).

194. The Court recalls that in a case concerning covert listening devices, it found a violation of Article 8 because there existed no statutory system to regulate their use and the guidelines applicable at the relevant time were neither legally binding nor directly publicly accessible (see *Khan v. the United Kingdom*, no. 35394/97, § 27, ECHR 2000-V). In *Malone*, cited above, §§ 69-80, it found a violation of Article 8 because the law in England and Wales governing interception of communications for police purposes was "somewhat obscure and open to differing interpretations" and on the evidence before the Court, it could not be said with any reasonable certainty what elements of the powers to intercept were incorporated in legal rules and what elements remained within the discretion of the executive. As a result of the attendant obscurity and uncertainty as to the state of the law the Court concluded that it did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities (see also *Liberty and Others*, cited above, §§ 64-70).

195. The Court considers it essential, in the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness (see *S. and Marper*, cited above,

§ 99, and the references therein). There are various crucial stages at which data protection issues under Article 8 of the Convention may arise, including during collection, storage, use and communication of data. At each stage, appropriate and adequate safeguards which reflect the principles elaborated in applicable data protection instruments and prevent arbitrary and disproportionate interference with Article 8 rights must be in place.

196. The provisions and principles of the Data Protection Act, the Data Protection Convention and Recommendation No. R (87) 15 are of some importance (see paragraphs 65-71 and 122-141 above). The Court emphasises in particular the terms of Principle 2.1 of the Recommendation, which excludes the open-ended and indiscriminate collection of data except where specific legislation is enacted to authorise such collection (see paragraph 130 above). The Court further draws attention to Principle 5 which sets out the need for a clear legal obligation or authorisation to communicate data to bodies outside the police in most cases, and the exceptional nature of any communication, in the absence of any such obligation or authorisation, intended to prevent serious and imminent danger (see paragraphs 133-135 above). Finally, the Court refers to the terms of Principle 7 of the Recommendation, which sets out a list of considerations to be taken into account when assessing the duration of any storage of data including rehabilitation, spent convictions, the age of the subject and the category of data concerned (see paragraph 138 above).

197. The Court also notes that the Supreme Court in *R (F and another)* recognised the need for a right to review in respect of the lifelong notification requirements imposed pursuant to sex offenders' legislation (see paragraph 120 above). In doing so, Lord Phillips noted that no evidence had been placed before the court that demonstrated that it was not possible to identify from among those convicted of serious offences, at any stage in their lives, some at least who posed no significant risk of reoffending. In light of the ensuing uncertainty, he considered that the imposition of notification requirements for life was not proportionate. The Court is of the view that similar considerations apply in the context of a system for retaining and disclosing criminal record information to prospective employers.

198. The Court observes that the recording system in place in Northern Ireland covers not only convictions but includes non-conviction disposals such as cautions, warnings and reprimands. A significant amount of additional data recorded by police forces is also retained. It is clear from the available guidance that both the recording and, at least, the initial retention of all relevant data are intended to be automatic. It further appears from the policy documents provided that a general presumption in favour of retention applies, and that as regards data held in central records which have not been shown to be inaccurate, retention until the data subject has attained one hundred years of age is standard in all cases. There can therefore be no

doubt that the scope and application of the system for retention and disclosure is extensive.

199. The Court recognises that there may be a need for a comprehensive record of all cautions, conviction, warnings, reprimands, acquittals and even other information of the nature currently disclosed pursuant to section 113B(4) of the 1997 Act. However, the indiscriminate and open-ended collection of criminal record data is unlikely to comply with the requirements of Article 8 in the absence of clear and detailed statutory regulations clarifying the safeguards applicable and setting out the rules governing, *inter alia*, the circumstances in which data can be collected, the duration of their storage, the use to which they can be put and the circumstances in which they may be destroyed.

200. Further, the greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data. The Court considers that the obligation on the authorities responsible for retaining and disclosing criminal record data to secure respect for private life is particularly important, given the nature of the data held and the potentially devastating consequences of their disclosure. In *R (L)*, Lord Hope noted that in 2008/2009 almost 275,000 requests were made for ECRCs alone (see paragraph 105 above). This number is significant and demonstrates the wide reach of the legislation requiring disclosure. As Lord Neuberger indicated, even where the criminal record certificate records a conviction or caution for a relatively minor, or questionably relevant, offence, a prospective employer may well feel it safer to reject the applicant (see paragraph 108 above; see also the views expressed in the Divisional Court in *R (Pinnington)*, at paragraph 87 above). The Court agrees with Lord Neuberger that it is realistic to assume that, in the majority of cases, an adverse criminal record certificate will represent something close to a "killer blow" to the hopes of a person who aspires to any post which falls within the scope of disclosure requirements (see paragraph 111 above).

201. It is against this backdrop that the lawfulness of the measures for retention and disclosure of criminal record data, and in particular the adequacy of the safeguards in place, must be assessed.

202. The Court reiterates that there is no statutory law in respect of Northern Ireland which governs the collection and storage of data regarding the administration of cautions. Retention of such data is carried out pursuant to the common law powers of the police, in accordance with the general principles set out in the Data Protection Act. In the absence of any statutory provisions, a number of policy documents which apply in Northern Ireland have been identified by the Government (see paragraphs 33-46 above). As noted above, it is clear from the MOPI Guidance and the ACPO Guidelines that the recording and initial retention of caution data are intended in

practice to be automatic. While reference is made in the MOPI Guidance to a review of retention after a six-year period, the criteria for review appear to be very restrictive. The Guidance notes that there is a presumption in favour of retention and the review schedule requires police to retain data in the category of "Certain Public Protection Matters" until the data subject is deemed to have reached one hundred years of age, regardless of the type or classification of data or grade of the intelligence concerned (see paragraphs 39-40 above). Any review in such cases seems intended to focus on whether the data are adequate and up to date. Pursuant to the ACPO Guidelines, it appears that data held in central police records are now automatically retained, regardless of the seriousness of the offence in question, until the person is deemed to have reached one hundred years of age. The ACPO Guidelines themselves explain that they are based on a format of restricting access to data, rather than deleting them. While deletion requests can be made under the ACPO Guidelines, they should only be granted in exceptional circumstances (see paragraphs 43-46 above). As noted above the examples given as to what constitute exceptional circumstances do not suggest a possibility of deletion being ordered in any case where the data subject admits having committed an offence and the data are accurate.

203. As for disclosure of caution data, at the relevant time there was no statutory framework in place in Northern Ireland which governed the communication of such data by the police to prospective employers. The disclosure of the applicant's caution data took place pursuant to the common law powers of the police, in accordance with the general principles set out in the Data Protection Act. The only policy guidance to which the Government have referred is contained in the ACPO Guidelines and the MOPI Guidance. The MOPI Guidance refers to the comprehensive system for disclosure in the employment vetting context set out in the 1997 Act, which did not apply in Northern Ireland at the time, and to general disclosure for police purposes under common law powers (see paragraph 58-59 above). The Guidance explains that in this context a balancing exercise must be carried out, but specific information regarding the scope of the discretion to disclose and the factors which are relevant to the exercise of such powers in the context of disclosure of criminal record information is not provided. Although the ACPO Guidelines make reference to a stepping down policy to limit access to data after a certain time period has passed, as noted above it appears that stepped down data were still intended to be available for disclosure in the context of requests for criminal record checks (see paragraphs 60 and 89 above).

204. Regarding any possible future disclosure of the applicant's caution data, the Court observes that there is now a statutory framework in place for disclosure of criminal record information to prospective employers. Pursuant to the legislation now in place, caution data contained in central records, including where applicable information on spent cautions, must be

disclosed in the context of a standard or enhanced criminal record check. No distinction is made based on the seriousness or the circumstances of the offence, the time which has elapsed since the offence was committed and whether the caution is spent. In short, there appears to be no scope for the exercise of any discretion in the disclosure exercise. Nor, as a consequence of the mandatory nature of the disclosure, is there any provision for the making of prior representations by the data subject to prevent the data being disclosed either generally or in a specific case. The applicable legislation does not allow for any assessment at any stage in the disclosure process of the relevance of conviction or caution data held in central records to the employment sought, or of the extent to which the data subject may be perceived as continuing to pose a risk such that the disclosure of the data to the employer is justified. In this regard the Court takes note of the offer made by the police in 2006 to add a comment to the applicant's record to the effect that the incident was domestically related and that in any vetting context she should be approached for an explanation (see paragraph 16 above). It is unclear whether such addition could have any place in the disclosure system envisaged by the 1997 Act given the automatic nature of the disclosure exercise in respect of caution data held in central records. In any event, the apparent preference of many employers for a clean criminal record certificate (see paragraphs 87, 108 and 111 above) would deprive such addition of any real value.

205. As regards specifically the fact that the retention policy changed after the administration of the applicant's caution, the Court notes that the applicant consented to the administration of the caution on the basis that it would be deleted from her record after five years. The Government have confirmed that this was the policy of the PSNI at the relevant time (see paragraph 25 above. See also the 1995 ACPO Code of Practice, paragraph 29 above). The police reply to the applicant's query in March 2003 is consistent with this understanding and confirmed that the caution would remain on her record until 17 November 2005 (see paragraph 10 above). The Court notes that in accepting the caution, the applicant waived her fair trial rights in respect of the offence in issue. It is not for the Court to assess whether she would, with the benefit of hindsight, have been in a better position now had she refused the caution. It must be recalled that the administration of the caution relieved her of the stress and anxiety of a potential criminal trial, which could have resulted in a custodial sentence had she been found guilty. However, the Court expresses concern about the change in policy, which occurred several years after the applicant had accepted the caution and which was to have significant effects on her employment prospects.

206. In the present case, the Court highlights the absence of a clear legislative framework for the collection and storage of data, and the lack of clarity as to the scope, extent and restrictions of the common law powers of

the police to retain and disclose caution data. It further refers to the absence of any mechanism for independent review of a decision to retain or disclose data, either under common law police powers or pursuant to Part V of the 1997 Act. Finally, the Court notes the limited filtering arrangements in respect of disclosures made under the provisions of the 1997 Act: as regards mandatory disclosure under section 113A, no distinction is made on the basis of the nature of the offence, the disposal in the case, the time which has elapsed since the offence took place or the relevance of the data to the employment sought.

207. The cumulative effect of these shortcomings is that the Court is not satisfied that there were, and are, sufficient safeguards in the system for retention and disclosure of criminal record data to ensure that data relating to the applicant's private life have not been, and will not be, disclosed in violation of her right to respect for her private life. The retention and disclosure of the applicant's caution data accordingly cannot be regarded as being in accordance with the law. There has therefore been a violation of Article 8 of the Convention in the present case. This conclusion obviates the need for the Court to determine whether the interference was "necessary in a democratic society" for one of the aims enumerated therein.

II. ALLEGED VIOLATION OF ARTICLES 6 AND 7 OF THE CONVENTION

208. The applicant complained under Article 7 of the Convention about the change in policy concerning retention of caution data. The Court of its own motion invited the parties to submit written observations on whether there had been a violation of Article 6 § 1 of the Convention.

209. The Court is prepared to accept that the complaints under Article 6 § 1 and Article 7 are arguable in the particular circumstances of the case and it therefore declares them admissible. However, it satisfied that the substance of the applicant's complaint concerning the retention and disclosure of her caution data has been addressed in the context of its examination under Article 8 above. It has found a violation of that Article as regards the system for retention and disclosure of caution data. In these circumstances it considers that it is not necessary to examine the complaint under Article 6 and Article 7 of the Convention.

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

210. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

211. The applicant did not submit a claim for just satisfaction. Accordingly, the Court considers that there is no call to award her any sum on that account.

FOR THESE REASONS, THE COURT UNANIMOUSLY

1. *Declares* the application admissible;

2. *Holds* that there has been a violation of Article 8 of the Convention;

3. *Holds* that there is no need to examine the complaints under Articles 6 and 7 of the Convention.

Done in English, and notified in writing on 13 November 2012, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Lawrence Early	Lech Garlicki
Registrar	President