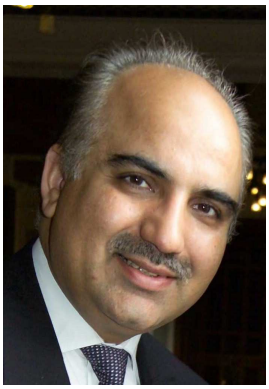

Dr Mirza Ahmad

LLD (*Hon*) Barrister

Called to the Bar : 1984

"Some key Data Protection issues"

Wolverhampton City Council
10th September 2013 Seminar

St Philips Barristers

The seminar will highlight some of the following issues…

1. **'Subject Access Code of Practice' -** The Information Commissioner's Office published this Code, last month. It's aim is to encourage best Data Protection Act 1998 (DPA) practice and it should be taken into consideration by all practitioners as the Information Commissioner and the Tribunal/courts will be mindful of it. However, a breach of the Code will not equate to a breach of the DPA, even though it has been published under the DPA This is an important document for all practitioners.

   Points covered in the Code include the following:

   - **Subject access is a 'fundamental right' -** "Enabling individuals to find out what personal data you hold about them, why you hold it and who you disclose it to is fundamental to good information-handling practice. The Data Protection Act 1998 (DPA) gives individuals the right to require you to do this." (p. 5).

   - **Requests made by social media -** Applicants can make subject access requests via the data controller's social media webpages/sites, such as Facebook, Twitter , LinkedIn etc accounts (p. 10).

   - **A child's right of access –** The data belongs to the child and not to any parent or guardian. The right may, of course, be exercised on the child's behalf by their parent or guardian (p. 11).

   - **Purpose or motive of the request remains not a relevant consideration –** (p. 20).

   - **Scope of the data controller's search obligations -** Considerations of reasonableness and proportionality are relevant. The code states that, whilst there are "no express limits" on the search obligation provided for under the DPA, data controllers are "not required to do things that would be unreasonable or disproportionate to the importance of providing subject access to the information", but the organisation must "make extensive efforts to find and retrieve the requested information", and requests cannot be refused simply because they are "labour-intensive or inconvenient" (p. 22).

   - **Commissioner's enforcement functions -** Enforcement notices will continue to be issued in cases where a data controller has failed to comply with its obligations under the DPA. However, a notice will not necessarily be served "simply because an organisation has failed to comply with the subject access provisions" and the Commissioner will consider whether the failure is likely to cause or has caused the data subject to suffer damage or distress. He will, of course, 'not require organisations to take unreasonable or disproportionate steps to comply with the law on subject access" (p. 53).

Contact details :
St Philips Chambers
mobile: 07429 335 090
mahmad@st-philips.com

London:
9 Gower Street,
WC1E 6BY

Birmingham:
55 Temple Row,
B2 5LS

Leeds:
7 Lisbon Square,
LS1 4LY

Dr Mirza Ahmad's

specialist expertise:

- **Public & Administrative Law**
- **Employment Law**
- **Commercial Litigation**
- **Personal Injury Law**
- **Direct Public Access**

Contact details :

St Philips Chambers

mobile: 07429 335 090

mahmad@st-philips.com

Clerks team:

Justin Luckman
Gary Carney
Sam Collins

Tel : 0121 246 7001

2. Other recent DPA issues and notable cases:

- **Aberdeen City Council** was fined £100,000 by the Information Commissioner's Office after the Council released details relating to the care of vulnerable children. The breach occurred after a council employee – who was authorised to access data relevant to her job remotely – accessed documents from her home computer. A file transfer program installed on the machine automatically uploaded four documents to a website, which included the minute of a core group meeting held in relation to a child; a LAAC Review minute and a child's plan. Sensitive information about several vulnerable children and their families, including details of alleged criminal offences, was released in breach of the DPA. The files were uploaded between 8 and 14 November 2011 and remained available online until 15 February 2012.

- **The Local Government Ombudsman** has given an undertaking to the Information Commissioner's Office after a bag - containing an encrypted portable media device and hard copy papers relating to eight complaints - was stolen from a pub. The ICO investigation revealed that there was a specific business requirement for the case papers to be removed from the Ombudsman's office environment and the LGO had – at the time of the incident – a policy on the security of information whilst in transit, but staff awareness of policies was "lacking due to the insufficient provision of training".

  Mandatory induction and annual refresher training in the requirements of the Act will be provided to all staff and there will be a recording of such training, including updates and monitoring, with oversight provided at a senior level against agreed KPIs to ensure completion. The LGO also agreed "to implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage."

- **Islington LBC** was fined £70,000 after it released personal details of more than 2,000 residents online following a freedom of information request. The ICO said the data breach arose out of a lack of understanding of pivot tables used in Microsoft Excel and other spreadsheet programmes. The ICO also said it was investigating a number of other authorities that had made similar errors. Islington said it would accept the fine and take advantage of the 20% early payment discount, bringing the total payable down to £56,000. Islington released three spreadsheets covering the work of its housing performance team. The documents contained the details of residents who were either tenants or had applied for council housing and included details of whether they had a history of mental illness or had been a victim of domestic abuse. The ICO investigation found that the council had been alerted to the problem shortly after the first spreadsheet was published, but failed to correct its mistake.

Dr Mirza Ahmad's specialist expertise:

- Public & Administrative Law
- Employment Law
- Commercial Litigation
- Personal Injury Law
- Direct Public Access

Contact details :
St Philips Chambers
mobile: 07429 335 090
mahmad@st-philips.com

Clerks team:
Justin Luckman
Gary Carney
Sam Collins

Tel : 0121 246 7001

- **Scottish Borders Council - The First-tier Tribunal (FTT**) has ruled that the Information Commissioner's Office should not have imposed a £250,000 fine on the Council in September 2012 after pension records for former employees were discovered in an over-filled paper recycling bank outside Tesco in Queensferry.

  It was found that a data processing company hired by the council had transferred the pensions records from hard copy files to CDs at the authority's request. The company then disposed of about 1,600 manual files in the post box bins at Tesco and at another supermarket in the town - one can only surmise that this highly irresponsible action by the company must have been in breach of its contract with the Council. The ICO, however, accused the Council of failing to put in place appropriate controls when outsourcing the destruction of confidential information.

  The FTT found that the arrangements with the contractor were "obviously defective" when it came to the obligations of a data controller under Schedule 1 Part 2 of the Data Protection Act when making contracts with a data processor. "Para 11(a) [of the seventh data protection principle (DPP)] required an informed choice of processor who should be able to provide sufficient guarantees in respect of technical and organisational security measures," the FTT said. "In place of this there was no more than a sincere but somewhat generalised attempt for reassurance some six years earlier."

  The FTT concluded that the arrangements made by the council for processing the pension records in July and August 2011 were in contravention of the Act and that it was a serious breach as the duties in relation to data processing contracts in paras 11 and 12 of schedule 1 were "at the heart of the system for protecting personal data under DPA. It is fundamental that the data controller cannot be allowed to contract out its responsibilities". Furthermore, the contravention was "not an isolated human error. It was systemic".

  However, the FTT went on to conclude that the contravention was not of a kind likely to cause substantial damage or substantial distress. "No doubt some breaches of the seventh DPP in respect of some data might be of such a kind," the FTT said. "In this case, it seems to us that the fact that the data processor was a specialist contractor with a history of 25-30 years of dealings with Scottish Borders carries weight. He was no fly by night. The council had good reason to trust the company."

  The FTT concluded that there was no liability to a monetary penalty in this case because, looking at the facts and circumstances of the contravention, whilst it was serious, it was not of a kind likely to cause substantial damage or substantial distress. The FTT delayed consideration of whether to issue an enforcement notice or take some other action to allow a conversation to take place between Scottish Borders and the ICO about the placing of data processing contracts and the training given to staff involved as "it may be possible for the parties to agree a way forward."

Dr Mirza Ahmad's specialist expertise:

- **Public & Administrative Law**
- **Employment Law**
- **Commercial Litigation**
- **Personal Injury Law**
- **Direct Public Access**

Contact details :
St Philips Chambers
mobile: 07429 335 090
mahmad@st-philips.com

Clerks team:
Justin Luckman
Gary Carney
Sam Collins

Tel : 0121 246 7001

The ICO confirmed it would not be appealing the tribunal's decision and the Scottish Borders will be repaid the original fine. A joint report between the council and the ICO on the progress made on improving processes and systems since the data breach - and a timetable for outstanding actions - will be submitted to the tribunal by 10 September.

- **NHS Surrey Trust** (dissolved at the end of March 2013, with responsibility now resting with the NHS Commissioning Board) was fined £200,000 after a "truly shocking" breach occurred with the sale of a computer containing more than 3,000 patient records. The accountable officer for information governance at NHS Surrey had not been involved in the sale arrangements and neither was there a written agreement with the company, although the NHS body did receive written assurances that the hard drives would be destroyed. Between 10 February 2011 and 28 May 2012 approximately 1,570 PCs with individual hard drives were collected by the company for destruction. One of the computer discs contained confidential sensitive personal data and HR records relating to approximately 900 adults and 2,000 children.

  The ICO investigation concluded that – in addition to having no contract in place with the new provider setting out its legal requirements under the Data Protection Act – NHS Surrey had failed to observe and monitor the data destruction process.

- **Stockport Primary Care Trust** (dissolved on 31 March 2013, legal responsibilities transferring to the NHS Commissioning Board) was fined £100,000 after it left 1000 personal data documents in boxes of waste left at a site it sold in 2011. The information included details of miscarriages, child protection issues and a police report relating to a child's death. The investigation also found that there had been two previous security incidents where personal data had been left behind in secure buildings owned by the trust. However, senior management at the trust had not been informed of these cases.

- The Information Commissioner's Office has also confirmed that it will pursue existing data protection cases against those organisations that have taken on accountability and the legal liabilities of now disbanded health bodies. The organisations affected have included the **Brighton and Sussex University Hospitals NHS Trust** (£325,000), **Belfast Health and Social Care Trust** (£225,000) and **Torbay Care Trust** (£175,000).

6th September 2013