BRIEFINGS ON INFORMATION LAW FROM AMBERHAWK ASSOCIATES

June 2014

INTRODUCTION

Amberhawk Associates are pleased to announce a set of **half day** and **full day briefings** which can be held at a location of your choice for any number of delegates. We do not object if you decide to share the cost with other organisations.

The sessions are appropriate for subject matter specialists as well as data protection officers. The objective is to explore information law issues in detail, within a specific workshop context, where questions can be asked and issues explored at any time. CPD points are available.

The fee for a half day briefing is £900 and £1,800 for a full day briefing. This fee excludes VAT and reasonable travel expenses).

HALF DAY BRIEFINGS

Data Protection and Human Resources Code of Practice

The Data Protection Act is discussed in the context of the following HR issues: fair processing notices & transparency: what should be declared on forms & websites; use and disclosure of medical personal data in HR; what staff can have access to which personal data; posting details of staff on the Intranet; opinions and disputed opinions (e.g. in appraisals and emails: accuracy, relevance); retention and disposal of personal data: archiving, and providing and getting references

There are sessions on: disclosure of staff details with consent (e.g. from payroll records); disclosure of staff details without consent (e.g. to external agencies; trades unions?); vetting of staff; surveillance and monitoring at work; consequences of rights of employees to personal data and the fact that the right of access might not apply.

We cover FOI expectations of public sector staff (e.g. re expenses claims etc); security obligations arising from HMG security classifications; data sharing of staff details outside the EEA and HR elements associated with procurement of equipment or use of data processors.

Data Protection and the Subject Access Code of Practice

All legal and procedural requirements associated with a Subject Access request to personal data (e.g. timescales, fees) and all problem areas (e.g. getting personal data from laptops, emails or archive, personal data that identify another individual).

Procedures associated with your chosen subject access exemptions (e.g. crime and taxation, research, information required to be made public; confidential references etc

All the above is set in the context of the ICO's Code of Practice.

Data Protection, Surveillance and the CCTV and Code of Practice

The course includes the following: Article 8 of the Human Rights Act, definitions, the lawful processing of images, fair collection notices and signage, camera siting, CCTV or surveillance of staff or at work, covert use of cameras and RIPA/DPA interface, Retention and disposal of images.

Disclosure of images (e.g. to external agencies), Misuse of images (e.g. CCTV cameras follow an attractive blonde) and rights of access to images.

Also considered is the ICO's and the Surveillance Camera Commissioner's Code of Practice that applies to, CCTV procurement and Privacy by Design initiatives and the importance of staff training.

If need be the course can cover, scope of the national security exemption and the crime prevention exemption, CCTV surveillance of demonstrations and ACPO's CCTV strategy

Information law for Schools - Data Protection and FOI

Contact us if you are interested in this course as the description is rather long and we draw up a detailed specification from a range of options

The overlap between Data Protection and ISO27002:2013, HMG Security Framework, NHS Toolkit and Local Government Data Handling Guidelines

The focus is the law underpinning the Seventh and Eighth Data Protection Principles. A review of data loss cases and how the Data Protection Act is enforced (Undertakings; Monetary Penalty Notices).

The course extends to key parts of ISO 27001 relate to obligations under these principles (e.g. policies and management structures; practices for securing data including access controls and encryption). Contracts with data processors. How this influences system design. Offences and other relevant law (e.g. Computer Misuse Act; rules of evidence, confidentiality).

For public sector bodies, the context of the training is likely to be the HMG Security Framework and Information Assurance Assessment instead of ISO 27001

Data Protection and Marketing Code of Practice on Online Marketing including PECR

A review of the definitions to identify when the direct marketing provisions of the Data Protection Act are engaged and a review of the definitions to identify when the Privacy and Electronic Communications Regulations (PECR) are engaged.

There then follows a detailed discussion (workshop style) with respect to the eight data protection principles in the context of: application forms, fair processing notices and what should be in a privacy policy re marketing purpose (including third party marketing); all forms of direct marketing and the right to object to marketing (includes PECR); market research and the research exemption; outsourcing the marketing function; behavioural marketing and the ASA database rules.

Also covered are important Tribunal and ASA cases of importance to the marketing function.

The Code of Practice and ICO Guidance is a focus of the training.

FOI - New rules on Datasets: Code of Practice

Contact us if you are interested in this course.

FULL DAY BRIEFINGS

Handling Subject Access Requests

This 1 day course captures all of the critical issues which organisations need to understand in order to deal effectively with Subject Access Requests (SARs).

SARs can create difficult challenges for data controllers, especially when they originate from disgruntled ex - employees, serial complainants, in the context of actual or prospective litigation or involve potentially wide ranging searches of substantial volumes of records.

This highly practical 1 day session will provide delegates with the necessary knowledge to effectively handle a SAR, recognise the pitfalls and create a SAR process and policy for their organisation.

The session includes:

- The legal right of subject access and the ingredients of a valid SAR
- The legal obligations on the data controller: deadlines; what to include in your response; when is it reasonable to seek clarification of the request?
- The role of the ICO Code of Practice on SARs
- Defining the scope of the search and whether to include archived and deleted information
- Dealing with wide ranging or voluminous requests
- Dealing with requests in the context of actual or prospective litigation: the extent to which you can refuse a SAR in this context
- How to deal with third party personal data
- The legal exemptions from the right of subject access
- Liaising with the applicant or the applicant's solicitors
- Handling a complaint or ICO investigation
- The ingredients of an effective corporate SAR Policy and process; the importance of SAR staff training
- Distinguishing between a SAR and other legal rights of access to personal data including: Access to Health Records Act and Access to Medical Reports Act, Access to educational records etc):

Data Protection in Social Care

This 1 day course is delivered jointly by a practicing data protection solicitor and a social care solicitor and is aimed at all those working in social care such as social workers, case workers and administrators.

It captures all of the critical issues which organisations need to understand in order to comply with the Data Protection Act (DPA) and the specific and unique challenges for those working in social care (adults or children).

The Information Commissioner's Office has not hesitated in enforcing the law against those working in this sector. Fines for breaches can be as much as £500,000 and will always be accompanied by adverse publicity and scrutiny.

Packed with practical examples which are relevant to what you do, this highly practical day will ensure delegates leave with a greater understanding of how the law applies to social care and equip them with an action plan for compliance for their organisation.

The session includes:

- Understanding what the DPA provides, who it applies to and when it is engaged in the context of social care
- The main requirements of the DPA with particular emphasis on the legal requirement to keep personal data secure;
- The technical and organisational steps you are expected to take to keep data secure; working remotely, encryption (when should you encrypt data or devices); BYOD
- Handling a breach of the DPA including dealing with an investigation from the Information Commission's Office, handling the media and service users
- Recognising and handling a Subject Access Request (SAR) under the DPA; requests from vulnerable adults or children; Gillick competency issues; Interface between the DPA and other legislation: exemptions from the right of subject access
- Requests for access to children's records from third parties including the Police, parents (including absent parents) and the court etc.
- Interface between data protection and the law of public interest immunity and when PII ought to be claimed so as to protect records from disclosure
- Data sharing and the ICO Data Sharing Code of Practice and related guidance
- Enforcement powers of the ICO including (but not limited to) the Monetary Penalty Notice
- Embedding compliance in your organisation: your action plan