Scottish Construction Safety Group

Minutes of the meeting of November the 23rd 2017

There were 19 members and guests present. Robert Bradford introduced David Freeland a senior policy officer with the Information Commissioners office (ICO) who has been employed by the ICO for almost 5 years. David was giving a presentation on the management of personal and sensitive data due to the changes being implemented by the new General Data Protection Regulations (GDPR) as laid down by the EU.

David began by advising that ICO is based in Manchester and has around 500 staff, there role is mainly to provide guidance, deal with data subject complaints and monitor, enforce and enforce data protection law. They can carry out audits, issue reprimands, order compliance, ban or limit processing and have powers of access. Results of audits are posted on the ICO website however the report is only posted with the written approval of the auditee. If approval is not given then this is stated on the web site. After the introduction of GDPR in May fines will increase to £20,000,000 or 4% of global turnover whichever is greater, although it should be noted that currently very few cases are taken to court.

The GDPR will be adopted by the UK and that the UK regulations were currently going through parliament. The new GDPR is an evolution on the existing Data Protection Act 1998 (DPA) which was a development of the 1984 Act. The changes mainly relate to the control of online personal information. If companies are following the practices set out in the DPA there should be little change required but they should regularly review the ICO web pages for further information and guidance. The regulations deal with personal information whether in manual or electronic form; personal information is any information relating to an identified or identifiable natural person. Special categories of personal information include race / ethnicity, political opinion, religious or philosophical belief, trade union membership, physical or mental health, genetic or biometric, and sexual life or orientation. Criminal convictions are also covered but not as a special category.

The management of data is the responsibility of the data controller, this post may be an organisation. The data controller is the person / organisation that decides on the purpose and means of processing the information. The data processors are people / companies employed by the data controller to do something with the personal data (the data controller makes all decisions on the actions, an example would be the outsourcing of payroll runs).

There are now six data protection principles (down from eight although the topics are all still covered.

1. Personal data shall be processed lawfully, fairly and in a transparent manner see https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. There can be more than one purpose and anonymised information can be used e.g. for research purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, make sure what is being asked is all relevant. If the information is not accurate then it should either be deleted or updated
4. Accurate and where necessary kept up to date. If the purpose has been fulfilled then the information should no longer be kept but consider insurance, legal and best practice requirements.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed. It may be necessary to make a business case for keeping information longer than necessary e.g. for keeping health information for research purposes.
6. Processed in a manner that ensures appropriate security of the personal data. The security arrangements will be based on the nature of the data, harm level, amount etc. Security should be provided for paper records and personnel should be trained in all security arrangements based on company procedures. If the information is required for a statutory purpose then consent is not required e.g. for health surveillance.

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ for full information.

Consent to gather the information must be freely given, this can be broken down in to two parts
Personal data – may be given verbally but a clear process must be followed
Sensitive data – explicit consent must be given

Please reply to Roy Jackson c/o BAM Nuttall, Glasgow Road Kilsyth G65 9BL
E mail roy.jackson@bamnuttall.co.uk

Further information can be found at https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/ The processing must be necessary. The data controller must be responsible for and be able to demonstrate compliance with the regulations. When systems are being designed or updated the principles and problems should be considered, this planning must be formalized in to a Privacy Impact Assessment (PIA) Guidance can be found at : https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf based on the DPA and at http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 for the GDPR it should be noted that the ICO will be publishing their own guidance on PIA's in due course. (*When preparing a PIA I would recommend telephoning the ICO for information they provide clear information and are very helpful RJ) The ICO produce various types of guidance generally in the form of Codes of Practice some of which have legal standing – check the initial pages for information.* When hiring a data processor a full audit should be undertaken to ensure that they are managing everything to meet the legal requirements, do not rely solely on compliance with certain standards. Draft guidance is available at https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/consultation-on-gdpr-guidance-on-contracts-and-liabilities-between-controllers-and-processors/

Organisations with more than 250 employees must keep a record of their processing activities. Smaller organisations must do so if their data processing activities present a risk to individuals, is not occasional or includes special categories of data or criminal conviction data. It may be necessary to carry out an informal audit to determine what information you hold.
The record must include:

- the name and contact details of the data controller (and the Data Protection Officer if one has been appointed),
- A description of the categories of data subjects and the categories of personal data
- The categories of recipients to whom the data have been or will be disclosed
- Details of any transfers to countries outside the EEA or to international organisations
- The time limits for erasure of the different categories of personal data
- A general description of the security measures

Any significant security breach should be reported to the ICO within 72 hours; this time includes weekends and holidays and the document can be completed online. The ICO will provide guidance on notification of a breach and may investigate formally. A Data Protection Officer (DPO) is required where the core activities of the organisation include regular and systematic monitoring of a large number of people, or the core activities consist of the processing of a large amount of special category data (including criminal conviction data). A DPO can be a member of staff or could be a contracted service. But they must have a good working knowledge of data protection and how it applies to the business. The position would be inappropriate for IT or HR personnel

Companies should check that Data Processors hold their information in the European Economic Area or if they are working outside the EA ensure that additional precautions are in place for security. Thes additional controls should also apply to back up information. Some countries such as Norway, New Zealand etc. are exempt from the requirements due to the standards that they apply. See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/transfer-of-data/

Individuals have the right to know why the information is being gathered; have access to the information; right to data portability; right to have the information erased, restricted or rectified if incorrect; prevent automated decision making. If a request for a copy of the information is made it should be provided within one month.

There are many guidance documents on the ICO website https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications and they can be contacted by telephone on 0303 123 1113 (Manchester) or 0131 244 9001 (Edinburgh). A monthly newsletter containing updates can be found at https://ico.org.uk/about-the-ico/news-and-events/e-newsletter/

Bob thanked David for his presentation. There was no other business. See the Group website http://www.scottishconstructionsafetygroup.org.uk/ for more details.

Dates of forthcoming meetings are
18/1/18 Pinsent Mason – legal update
15/2/18 22/3/18 19/4/18 24/5/18
Topics including – lifting, occupational health (physicians view), toxicological information on drug and alcohol testing and fire risk assessment, will be matched to dates shortly.

Please reply to Roy Jackson c/o BAM Nuttall, Glasgow Road Kilsyth G65 9BL
E mail roy.jackson@bamnuttall.co.uk