Implementation of GDPR in a Large UK and European Business

Rob Fowler, Technical Services Planning Manager, Dpd Group

- GDPR replaces the Data Protection Act on 28 May 2018. All organisations processing personal information of UK/EU residents will have to comply. GDPR will apply post-Brexit.
- The Information Commissioner's Office (ICO) is the regulator responsible for ensuring compliance, with the power to impose fines – which will be based upon the scale of the breach and the turnover of the business.
- GDPR applies to any information an organisation holds that could ultimately identify an individual. This is known as an Information Asset.
- Organisations (Information Asset Owners or IAO's) need to establish, for example, whether the Information Asset has a value or is of use to them, and whether there would be financial or legal implications if it could not be produced when requested.
- Individuals have a "right to be forgotten" – which means anything held on that person has to be removed upon request from that individual. So, you need to know where information is stored, what is being stored , what and how it is removed (in line with legal retention periods), who has access to it and why.
- Organisations will need to review all data held, and also appoint a responsible person to act as IAO and create an Information Asset Register (IAR) - ensuring it is up-to-date, compliant and comprehensive and lists all the types of records held (hard copy or computer files).
- Tighter controls need to be in place where data is held on external drives/data sticks. Also, where information is outsourced to other organisations (eg solicitors, sub-contractors, claims handlers) you will need to ensure that they too are GDPR compliant.
- If in any doubt, declare any information held on the Register, rather than risk non-compliance.
- The ICO must be informed immediately if you have any data stolen..