

## TRADE.

# DON'T GET CAUGHT OUT ON DATA PROTECTION

THE INFORMATION COMMISSIONER'S OFFICE NOW HAS THE POWER TO LEVY FINES OF UP TO £500,000 ON COMPANIES THAT SERIOUSLY BREACH THE DATA PROTECTION ACT. JIM WATSON, MD OF CONFIDENTIAL DATA DESTRUCTION SERVICE SHRED EASY, AND DANIEL BERKE, A FRAUD SOLICITOR AT LEWIS HYMANSON SMALL, DISCUSS THE IMPLICATIONS FOR CLOTHING SUPPLIERS

### Clothing the nation's workers

There are approximately 11 million workers who wear uniforms in the UK, and many of these are serviced through fully-managed contracts that see suppliers store a significant amount of data about wearers. This includes size details, special requirement information, place of work and length of service, all of which must be handled securely and responsibly by the supplier.

This information is often stored in wardrobe management systems. These enable accurate and efficient management of accounts, as well as allowing wearers to order their own uniforms, but the sheer amount of data they can hold means they need to be carefully and securely managed.

### Data management

Clothing suppliers must now be more security conscious than ever and legally must destroy all employee data to do with sizing and addresses.

To avoid breaching legislation all companies must destroy personal employee information once a worker has left a company. And if these details have been shared with overseas partners during the course of the contract, these partner companies must also destroy any employee data they have on record.

### Data theft

One of the reasons behind the tough legislation is data theft, and this is

a threat to businesses of all sizes.

The root of the problem lies with the ingenuity and adaptability of the criminal fraternity. Identity theft and fraud has become one of the fastest growing crimes, increasing by 36 percent last year. To give an indication of the scale of the problem, the losses are equivalent to £631 a year for every household in Britain.

This means that anyone handling personal details, credit card information, addresses, bank account details, etc. for another party, is bound by law to protect this data. In the electronic age, when such information can be circulated around the planet in a microsecond, the risk is constant.

### Confidential data crime

Recent cases of employees stealing data from employer's confidential files, and cases of confidential data being left in the street, only serve to exacerbate fears. The prime reason for the exponential growth in the crime is the casual way many of us have customarily dealt with potentially damaging data. We leave files lying around, slip them into unlocked filing cabinets and take old PCs and discs to the dump, with the hard drives bulging with confidential data.

In short, the nature of business means dealing with confidential data. Companies absolutely must review and, if necessary, revise the way they deal with this risk.

The clear answer is to change working practices to make life as difficult as possible for the criminally inclined. All current documents

containing sensitive information should be kept under lock and key when not in direct use. Store rooms should be accessible only to the most trusted staff. Think about where or when a customer, dishonest employee, temporary worker, cleaner or maintenance tradesman could access written or electronic data. Then act to remove that possibility.

### Threats

If threatened with a penalty the Information Commissioner will take a business's turnover, sector, size and the data breach into account before considering a fine. This will be determined by carefully considering the circumstances, including the seriousness of the data breach, the likelihood of substantial damage and distress to individuals, whether the breach was deliberate or negligent, and what reasonable steps the organisation has taken to prevent such breaches

### Fines

The heavy fines are a warning to all organisations to protect and destroy confidential data securely and are part of the ICO's overall regulatory toolkit. They're not afraid to use it.

The answer is to monitor and control the use and flow of data much more carefully, take extra security precautions and, perhaps most importantly, to get some expert advice about disposal of your printed matter, IT equipment and data stored on all manner of tapes, discs, micro

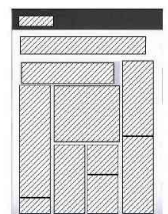
chips and USB sticks.

### Destroying the evidence

These materials can now be destroyed highly effectively and efficiently. Perhaps equally as important, these materials can also be recycled, enabling organisations to fulfill their environmental obligations at the same time as protecting themselves from prosecution and their clients and stakeholders from risk. A single visit from a state-of-the-art shredding truck can completely dispose of a mass of collected confidential data.

Every clothing business has a responsibility to shred their confidential documents and electronic data. Confidential data in the wrong hands can end in theft, a fine or the downfall of a business. ■

For more information about the data legislation and potential penalties see [www.ico.gov.uk](http://www.ico.gov.uk). For information about Shred Easy's data destruction services see [www.shredeasy.com](http://www.shredeasy.com).





Wearer details stored in wardrobe management systems must be destroyed if the employee leaves the client company.