



NSDR

National Staff Dismissal Register

National system to reduce losses attributed to staff

Background

In the last six years, staff theft and fraud has cost the retail industry more than £2.9 billion, with an average yearly loss of £497 million*.

Whilst individual retailers and businesses kept records of staff who were dismissed for gross misconduct (e.g. theft and fraud) there was, until the development of the National Staff Dismissal Register, no common shared database which could alert businesses to problem applications. It is known that a number of individuals exploit this situation and as a result businesses unwittingly employ staff who have been dismissed for dishonesty from similar organisations. The employment of such a person introduces a risk into the business that if unchecked, may result in serious losses.

The Register

The National Staff Dismissal Register (NSDR) is an Action Against Business Crime (AABC) initiative to reduce losses attributed to staff dishonesty. AABC is a subsidiary company of the British Retail Consortium and was established to help businesses better protect themselves against crime.

The database holds details of individuals who have been dismissed (whether prosecuted or otherwise) or left the company whilst under suspicion of:

- Theft or attempted theft of money, merchandise or property from the Company, its suppliers, staff or customers.
- Falsification or forgery of documents.
- Fraudulent acts resulting in the obtaining or intention of obtaining money, assets, services or information which would otherwise be denied.
- Causing a loss to the Company or another party (e.g. Supplier).
- Causing damage to Company property.

To help meet the challenges of compliance with the Data Protection Act, when adding records to the system, users are required to confirm that the reason for dismissal conforms to one of the above definitions.



action against
business crime
by business - for business

Data Protection

Hicom have extensive experience in the area of Data Protection and Confidentiality. We continue to monitor changes in legislation that may impact on how our customers work with our systems.

The Data Protection Act 1998 (DPA) regulates the use and handling of information (personal data) processed by computers and information held on manual records. It provides a framework for the sharing of information by establishing data protection principals. The purpose of the DPA is to make provision for the regulation of the processing of information relating to individuals including the obtaining, holding, use or disclosure of such information. All processing must be in compliance with the provisions of the act and in the event of non-compliance the Information Commissioner may take enforcement action.

As a member of the NSDR a Company is considered a Data Controller. Particular obligations are placed upon Data Controllers which must be complied with to ensure that there is no breach of the requirements of the DPA. It has therefore been important to restrict the content of the NSDR to information about individuals who have been dismissed for fraud or theft (or attempts) rather than any wider criteria.

In order to comply with the Defamation Act 1996 each member of the NSDR will be required to ensure that there is sufficient evidence to support their interpretation of the dishonest event when adding or updating a record on the system.

Consideration is also given to the Human Rights Act (1998) and the Freedom of Information Act (2000) with regard to recording of personal information, and the potential sharing of data with a public authority.



NSDR datasheet

"An average 32% of losses can be attributed to staff theft and fraud".

Mike Schuck (Action Against Business Crime)

