NSDR

National Staff Dismissal Register
National system to reduce losses attributed to staff

NSDR datasheet

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 Home Office supported body set up 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.

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.

Hicom Business Solutions

action against business crime
by business - for business

> **"An average 32% of losses can be attributed to staff theft and fraud ".**
> Mike Schuck (Action Against Business Crime)

System Access

Access to the system is strictly regulated to ensure data is secure and confidential. Every log-in is recorded and your nominated system adminstrator has the ability to review all database access through a summary activity screen.

Validation

The system validates records on entry to ensure minimum data requirements have been met.

Search Criteria

NSDR provides the ability for a user to search for an individual using any of the key identifying fields: Surname, Forename, Date of birth, National Insurance Number, Address and Previous employer.

The system returns a list of matching individuals based on the search criteria provided. The user may then select the record to view the details in full.

Photographs

To simplify identification, the system provides the ability to upload one or more images of the employee for association with the staff record. Images are automatically converted to web efficient format by the system for optimum storage and retrieval.

Personnel Record

When viewing a personnel record, the system requires the user to confirm if the person viewed is an applicant or not. If a confirmed match is made then the system requires the user to enter the employment status of the individual.

Audit Trail

Every time any record is added, accessed, edited or deleted the system records the user and date/time of the event. The audit trail cannot be amended or deleted.

In the event that a participating member leaves the scheme the existing data is retained for audit purposes and then deleted after three years.

* Source: British Retail Consortium crime figures (2005).

Reports

The NSDR system provides a reporting facility to produce a hard-copy report of all personal details held on an individual, should a Company choose to share this data with the said individual.

The system will also provide statistical reports on:

- Number of records on system.
- Number of searches conducted (by user) and average per month.
- Number of confirmed enquiries.
- Matched records requiring employment status confirmation.

Business Benefits

- Cost saving through reduced losses.
- Time savings resulting from a more efficient recruitment process with potentially lower staff turnover.
- Informing an applicant that they will be checked against a national register may result in dishonest applicants withdrawing their application.
- A dishonest employee will be added to the system on the day they are dismissed, with the reason for their dismissal.
- The system acts as a deterrent to existing staff against dishonesty.
- Improvement in perceived quality of business environment by employees and customers.
- With all members of the NSDR expected to add data, the value of the resource will build with additional users.

Security

The system is provided through a secure web based portal. The application uses a Secure Sockets Layer (SSL) to protect data access and encrypt log-in.

The application and database will be held on separate servers with firewall and Internet Protocol Security (IPSEC) separating application and data for further security.

System Maintenance & Support

The application is hosted by Hicom, so no maintenance is required by the user. Hicom is responsible for the day-to-day maintenance of the NSDR server including ensuring all data is backed up regularly and the latest security and application patches are applied. The NSDR ensures physical security and resilience of the server and server connection.

Hicom Business Solutions

Microsoft
C E R T I F I E D
Partner