



Datascrambler

Datascrambler helps to protect sensitive personal data and ensure legislative compliance by eliminating the need to use real citizen data for testing or training purposes.

The recent HM Revenue and Customs high profile loss of 25 million child benefit claimant details and series of data losses across both central and local government have served to remind organisations of their responsibility to safeguard personal data.

With revenues, benefits and housing systems containing highly sensitive personal data, there is a fundamental need to respect customers privacy and ensure that customers are protected from identity theft.

In their publication 'Guidelines for the use of personal data in systems testing' endorsed by the Information Commissioner, the British Standard Institute advises against the use of real customer data in test systems.

In addition to security risks, organisations using real customer data in a test environment are in breach of the Data Protection Act unless they have obtained permission from those customers.

Risks associated with using real data in a test system

Greater risk of information leakage

Test and training systems are usually far less vigorously monitored than live systems. It is common practice for a wider range of staff to have access to the system often with greater access rights than available in a live system.

Prosecution

The second principle of the Data Protection Act 1998 forbids organisations from using data beyond the purposes for which it was obtained. Organisations using real data for test and training purposes are at risk of breaching the act and prosecution, which could lead to seven-figure fines.

Public Relations damage

Organisations seen to be handling personal data inappropriately face damage to the public perception of the organisation. This can affect customer willingness to trust the organisation with their personal data often making it harder to deliver services.

Errors affecting customers

Test and training systems are often linked to live systems such as printing and e-billing solutions. As such, there is a risk of sending inaccurate "dummy" data to real customers, leading to potential significant customer service problems.

The Datascrambler uses a variety of techniques to "scramble" key data fields and tables within test databases to destroy live data. The result is a database identical in size and structure to the original but containing fictitious data. The new database can then be used as normal for testing purposes but without the risks associated with using real data.

CAPITA



How the Datascrambler works

The Datascrambler uses a variety of industry standard techniques including (but not limited to):

Shuffling

Involving use of complex algorithms to move data values such as names from one record to another

Masking

Involving overwriting sensitive data, for example that in notepads, with 'X's

Substitution

Replacing data such as email addresses with software generated values.

The exact technique used by the Datascrambler will vary depending on user selection, the interaction that the data being scrambled has with other parts of the system and any validation that applies to the field.

Default settings are provided to ensure customers can use the solution rapidly; however, the solution is also fully customisable enabling customers to implement their own policies.

The Datascrambler can be used to scramble data within Capita Revenues and Benefits and Capita Housing. A similar facility is available within the Capita Payment Management product set. For users of that solution, further details are available via your Capita Payment Management Account Manager.

"We are using the Data Scrambler and found it quick to install and easy to use. It has helped us with GCSX compliance and has effectively made all the data in our training database anonymous without compromising usability."

Jon Hopewell, Systems Support Manager
London Borough of Barking and Dagenham