Lexis® Visualfiles™ Obfuscation Tool

How do you ensure your Visualfiles systems aren't putting your clients' personal data at risk?

The Lexis Visualfiles Obfuscation Tool lets you easily mask sensitive data in copies of your Visualfiles production system. It enables your developers to safely build and test new workflows in fully functioning non-production test and development environments – without exposing your business to the risk of data loss or data protection fines.

Reduce your exposure to risk

By keeping sensitive and personal data out of non-production test and development environments, the Obfuscation Tool helps you to:

- Avoid breaching data protection legislation and incurring hefty fines. Copying personal data into non-production environments could potentially breach the EU GDPR/UK data protection laws.
- **Reduce the impact of cyberattacks.** Non-production environments are often more vulnerable to cyberattack than live systems. Hackers know this and so make them a target. You can reduce the financial and reputational risk of a successful attack on any of your non-production Visualfiles environments by keeping sensitive and personal data out of them.
- **Neutralise the danger of accidentally executing workflows.** If your non-production environments contain real personal data, developers run the risk of triggering incorrect invoices, letters or emails to actual individuals while testing workflows. This could easily cause damage to your brand that can be avoided by masking or replacing personal data.

Protect sensitive and personal data

As you create non-production environments, the Obfuscation Tool lets you quickly and flexibly mask, blank or replace data. You can:

- **Identify personal data in Visualfiles faster.** The configuration utility flags where personal data is likely to be present in Visualfiles making it easy for you to quickly identify the data you need to protect.
- **Specify precisely how to treat sensitive or personal data.** You have complete control over how you choose to blank, mask or substitute data.
- **Pull in dummy data from external datasets.** When your developers want to work with data that's similar in kind to your live system, the Obfuscation Tool lets you easily replace actual with realistic-looking dummy data. This helps your developers ensure new functionality is robust without risking the use of actual data. You simply specify the external data source to pull in data from and which fields you wish to be replaced.

Free up your Developers' time

Without the Obfuscation Tool your developers would have to develop scripts and processes to protect data when creating a non-production environment. With it, your developers have that time freed up to work on
other projects. And fully populated non-production environments can be created without delay.

Create multiple non-production environment

You can create as many non-production environments as you need. And you can use customised settings for each one. The Obfuscation Tool lets you mask sensitive and personal data exactly as required for each non-production environment you're running.

No Visualfiles upgrade required for most users

The Obfuscation Tool is compatible with all recent versions of Visualfiles.

Contact us for more information on how the Obfuscation Tool can help you to protect sensitive data against breaches and reduce your exposure to risk when developing with Visualfiles.

If you would like to find out more about the Obfuscation Tool, please contact your Account Manager today.

Lexis® Visualfiles™

LexisNexis®

Visit: www.lexisnexis-es.co.uk Tel: +44 (0)113 2262065 Email: salesinfo@lexisnexis.co.uk