Welcome

Welcome to the GDPR newsletter for users and partners of Datafile Software.

If you have any suggestions for topics you would like to see covered in future newsletters please contact the team via the email address below.

Terry Moore

Managing Director
Datafile Software Solutions Limited

Contact Details

Telephone
01772 816 514

Facsimile
0845 643 2624

Email
office@datafile.co.uk

Website
www.datafile.co.uk

Follow us on Twitter

Subscribe to our YouTube channel

Knowledge Base
http://kb.datafile.co.uk/

Address
Datafile Software Solutions Ltd
Windgate Lodge
1c Tarleton Office Park
Windgate
Tarleton
Lancashire
PR4 6JF

General Data Protection Regulations

What is the GDPR?

The General Data Protection Regulation is a new set of EU regulations set to come into force, as a replacement to the existing Data Protection Act.

When Does it come into force?

May 25th, 2018.

Who Does It Concern?

It's the rules and regulations for personal data protection, and every organisation within the EU must comply.

What is meant by Personal Data?

Personal data refers to data, whether true or not, about an **individual** who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access.

What about Brexit and Article 50?

Organisations from within the UK will still have to comply with the regulations when they come in. The UK will still be in the EU in May 2018 so will be still held to their rules. The Government have confirmed that they will be implementing GDPR regardless of Brexit.

Who Needs to Know About it?

Everyone in the organisation, or company. Business owners need to ensure that they have given their employees clear guidance on the regulations and procedures that need to be in place for due diligence.

What Types of Privacy Data does the GDPR Protect?

- Identity information such as name, address and ID numbers
- Web data such as location, IP Address, cookie data and RFID tags
- Health and Genetic Data
- Biometric Data
- Racial or Ethnic Data
- Political Opinions
- Sexual Orientation

The Key Requirements

Privacy

All privacy notices (e.g. on your website) that you issue need to be audited and amended so that they comply with new guidelines.

Accuracy

Any personal data and information held needs to be accurate and up-to-date. Any organisation who shares data with another organisation, must make clear any changes made to the information contained within. If changes to data are made, you need to record these changes, to keep an accurate record / trail of the amendments.

Access

Individuals are set to have much greater access to any of the personal data that an organisation stores on them. They will legally be allowed to view this data in entirety, as well as making it clear on the levels of profiling or direct marketing they will permit. Individuals can also request deletion of all data contained upon them, with organisation procedures and processes altered to ensure this is adhered to post-GDPR enforcement.

Consent

Ensure that your policies are in full compliance with new GDPR laws on granting clear consent for individuals to access their data

Security

GDPR will enforce ever stricter rules upon organisations to ensure that they are taking all reasonable measures to guard against data theft, loss, or other breach. Clear evidence must be shown that you have taken diligent measures in regard to security software, physical security, and other aspects such as disaster recovery plans.

If you do suffer a breach, then it is your duty to let the Information Commissioner's Office (ICO) know at the earliest possible moment.

Your terms of service need to reflect the seriousness that you take your obligations to security.

Responsibility

Organisations will be required to have an appointed Data Protection Officer to oversee all obligations and responsibilities. 3rd party or external officers are permitted, subject to approval.

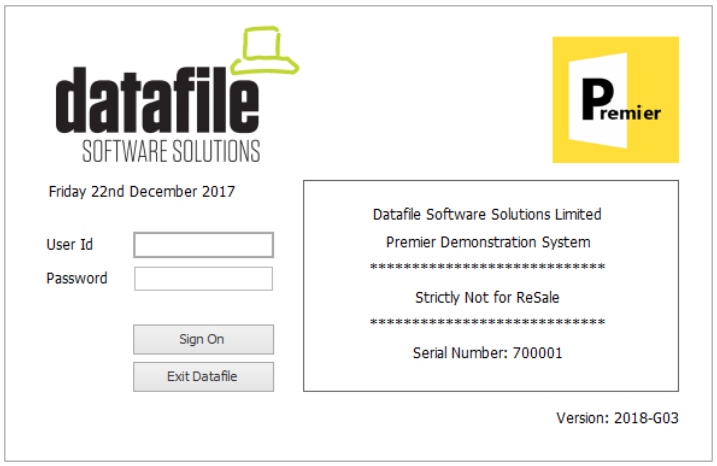
Obviously, there's more detail into which you'll need to delve depending on your own circumstances with regard to information storage and access, but these are the key issues that need to be adhered to and in place by May 25th 2018. It's likely that many of these procedures are already happening within the business but please check your policies, procedures, and safeguards to make sure they comply and everyone in the business understands the implications.

Datafile Software Solutions Limited
Windgate Lodge, 1c Tarleton Office Park, Windgate, Tarleton, Lancashire PR4 6JF
Tel: 01772 816 514 Email: office@datafile.co.uk

Considerations for your Datafile System

Access to the Datafile System

Primarily the data on your Datafile system can only be viewed or amended through the Datafile application. Exceptions to this may arise however if data is exported to a third-party application, or viewed through SQL e.g. with the Excel RTD module.



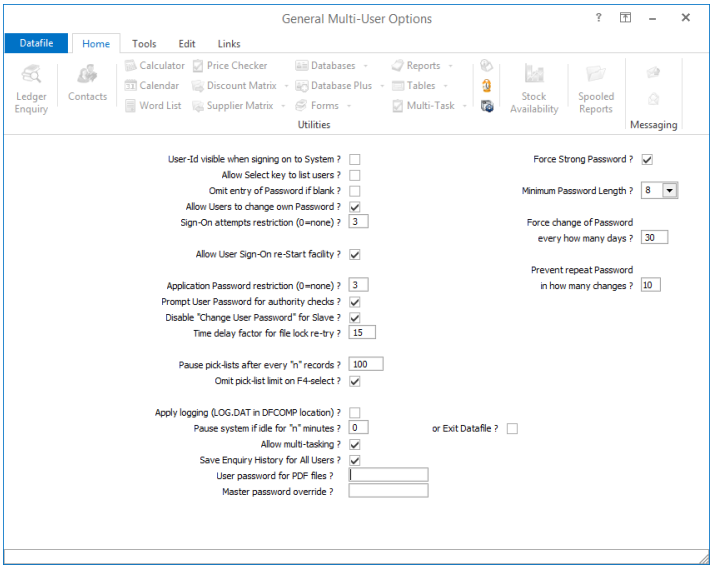
You should review your system security starting with User-Id's and Passwords and check the following:

- Ensure user passwords are updated regularly.
- Password Complexity is set.
- Remove any leavers from your list of allowed user-ids.

Each user carries an authority level that controls the areas of the system that the user is allowed access to. Review these settings to ensure users only have access to areas of the system required for their role. Review the Security & User Manager, Application and menu settings to verify that sensitive application options (payroll for example) are restricted.

All the password and system protection settings come to nothing though if users leave their Datafile session logged in when they are away from their desk. Consider using the Pause function where after a period of inactivity the screen is locked requiring password entry to resume. Additionally, the system can automatically log the user out after it detects a set period of inactivity.

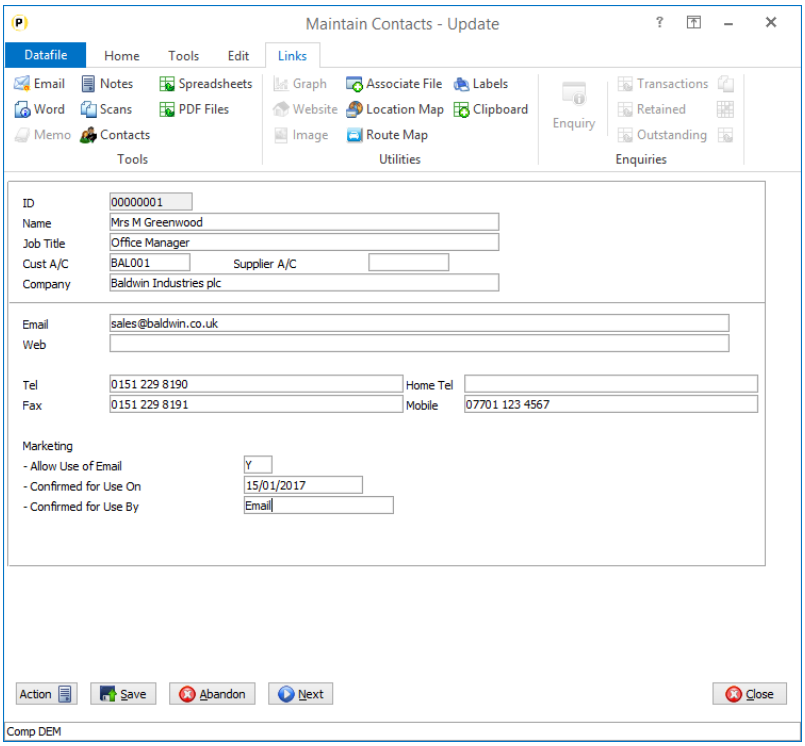
Access to the Datafile system can only be from a terminal with links to the Datafile program. Review who has access to terminals from outside the organisation and check whether users have installed any software to work remotely, are these passwords secure and updated regularly, is such software removed or passwords changed when employees leave?



Datafile Software Solutions Limited
Windgate Lodge, 1c Tarleton Office Park, Windgate, Tarleton, Lancashire PR4 6JF
Tel: 01772 816 514 Email: office@datafile.co.uk

Data Stored within Datafile

GDPR relates to data for individuals. You should review the type of data you hold for individuals. You are likely to hold data for individuals within your customer, supplier or payroll ledgers plus associated contact and order files – whether that's contact name and address, email address, mobile and telephone numbers etc.



Is this data required for business operation – if not consider removing it.

Is this data used internally or shared with outside agencies for marketing purposes? Do you have clear logging procedures to monitor requests for removal/update, logging actioning of this request, following this request up with marketing agency, and so on. Are you logging/recording confirmed acknowledgements that such information can be used for these purposes?

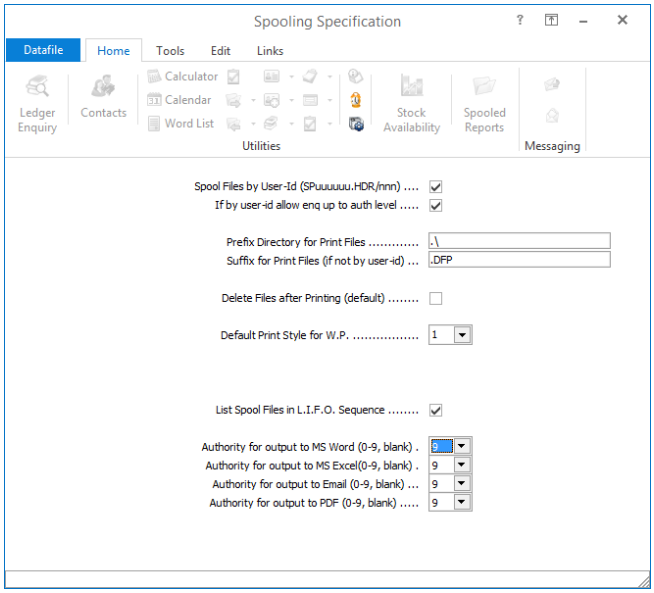
What about financial data – you should never hold credit/debit card information within Datafile databases but what about bank account data you may hold for suppliers, customers or employees. Who can view/update this data, do you record who has accessed or updated this data?

Reporting from Datafile

Datafile data can be output to other applications, whether that's using our SQL tools or generating a report listing to Excel, Word or PDF.

When using our SQL tools ensure that the SQL database is secure and has controlled access. Consider creating views for just the required data rather than the full database table.

Also check authority levels for which users can send reports to Word / Excel / PDF.



Datafile Software Solutions Limited
Windgate Lodge, 1c Tarleton Office Park, Windgate, Tarleton, Lancashire PR4 6JF
Tel: 01772 816 514 Email: office@datafile.co.uk