OpenPeople & the General Data Protection Regulation (GDPR)

What does GDPR mean for OpenPeople users?

On 25th May 2018, the General Data Protection Regulation (GDPR) will be enforced across Europe, replacing the Data Protection Directive 95/46/EC and therefore the Data Protection Act 1998.

Although this law comes from the EU, it will have a global impact. It will affect any business holding personal data relating to a living individual which could be customers, prospects or employees based within the EU. Despite Brexit, the UK will still need to comply with this legislation.

If organisations neglect to comply with the new GDPR, they can be fined up to €20m or 4% of their global annual turnover. It is therefore vital that organisations begin preparing for the new regulation now.

Although GDPR came into force in April 2016, organisations were given until May 2018 to become compliant. However, our recent annual Trends Survey revealed that 38%* of commercial organisations don't know if GDPR affects them. If you are one of those 38% of businesses, now is most certainly the time to get to grips with the legislation.

OpenPeople users will need to think about the different types of data which is stored within the system and what processes they need to put into place using the solution to ensure this data complies with the GDPR before May 2018.

How can Advanced help?

At Advanced, we are committed to ensuring that our customers are in the best position possible to meet the new GDPR requirements. To address this, we have invested our time in upskilling our product experts who have worked on significant developments in OpenPeople to assist our customers on their journey to compliance.

OpenPeople has numerous areas of Personally Identifiable Information (PII) which users of the system will need to ensure is compliant with new standards. In March 2018 we released a new GDPR module will enable users to put the right processes in place within the system with ease, including; a new PII flag at a field level, new retention rules table and custom reporting to identify imminent retention 'breaches.'

The GDPR module for OpenPeople will include:

> **Personally Identifiable Information (PII) Flags**

PII data is one the fundamental parts of the GDPR legislation, and these flags enable users to identify the relevant data. To enable management and control, the GDPR pack provides a set of programs that allow fields to be added to the already extensive list that will be set during the install by the Advanced Professional Services team.

The programs cover:

Field Maintenance

This allows any field to be classified as PII data and expects a set of rules to be attached to the field.

Anonymisation & Retention Rules

This is where you define the type of anonymisation you wish to be applied to the field e.g. retention date. They form the basis of the lookup table available in the field maintenance screen.

Trigger Rules

These are similar to the anonymisation rules but they allow the setting of a trigger point for the countdown from the retention date i.e. a supplier or employee recors might be set to trigger at a point in the future based on the date of the last payment.

> Anonymisation

Recital 26 of the GDPR defines anonymised data as "data rendered anonymous in such a way that the data subject is not or no longer identifiable". This definition emphasises that anonymised data must be stripped of any identifiable information, even by the party that is responsible for the anonymisation.

In order to allow our customers to easily manage their responsibilities under the new GDPR legislation, the GDPR pack provides one place to control the detail of any data anonymisation requirements. This option is controlled by a parameter setting making it company specific, allowing the GDPR functionality to be turned off for companies within the group where it doesn't apply.

> Retention Management

The GDPR sets up additional requirements around retention of personal data compared to the Data Protection Directive. Within the OpenPeople pack, the system states how long data can be held, giving users full visibility of when data needs to be removed from the system.

> Subject Access Request (SAR) Reporting

The capability to report on SAR and breached data reports is provided within the GDPR pack.

To run the Individual Report there is a selection window. This allows for up to four different levels of criteria with which to define the correct subjects for the report. It allows a field to be specified and then the search data to be entered.

The options for running the reports are all detailed on the screen, including whether this is to be run in the foreground or background and the format for the report to be delivered in which can be XML or HTML.

Where the request has come from an individual and the right to be forgotten box is selected, providing the report is run in update mode the data is anonymised.

The breach report is similar, but when run in update mode all the data that is exceeding the retention days on file in respect of the trigger field will be anonymised.

> Hard Deletes

Hard Deletes are available as standard within OpenPeople as part of archiving and purge functionality. Consultancy is available to assist users with this.

> Additional functionality for OpenPeople users

Encryption Support

This is another key part of the legislation that is committing 'Data Owners' to provide care in the handling and distribution of PII data. The laws specifically cover data at rest and in transit. We will be certifying and providing Progress Transparent Data Encryption (TDE) encryption tools that can be used by customers - although this is at an additional cost to the GDPR pack as it is supplied by Progress Software. OpenPeople, through the use of Progress TDE, includes both policy tools and a secure encryption key store kept apart from the database. Leveraging the authentication, authorisation and auditing functionality inherent in Progress® OpenEdge® and the additional Advanced Business Language (ABL) security features, TDE provides seamless data protection.

- On disk
- In backups
- In binary dump files
- By supporting encryption ciphers such as AES, DES, DES-3 and RC4

Through the use of Progress OpenEdge TDE, OpenPeople provides a solution that can fulfil the 'while at rest' component of an end-to-end application data privacy system, providing customers with peace of mind over security of data integrity.

For customers using SQL version of OpenPeople, there are inbuilt SQL server encryption tools available which can be used by customers. This provides peace of mind over security of data integrity - please speak to your SQL DBA for further details.

Find out more

For more information on how we can help you on your journey to compliance using OpenAccounts, please contact your account manager.

More information

w oneadvanced.com
t +44(0) 8451 605 555
e hello@oneadvanced.com

Ditton Park, Riding Court Road, Datchet, SL3 9LL