General Data Protection Regulations – Global 3000 V6.0 product update

Introduction

As of 25th May 2018, General Data Protection Regulations (GDPR) come into force within the European Union (EU). GDPR strengthens and unifies data protection for individuals within the EU and prescribes certain obligations on the export of personal data outside the EU.

This document outlines additional functions and tools that are available within Global 3000 (V6.0) to assist customers as they consider their GDPR compliance strategy.

This document does not in any way attempt to offer legal advice and guidance in respect of the regulations or how they should be implemented within an individual business. GDPR compliance is the responsibility of each individual business and suitable legal guidance should be sought as required.

Principles of operation and use of these features

The functions and tools described below enable customer and supplier contact records to be updated with data protection settings (which are used to determine their GDPR status). In addition, they can also be used signal that contact data is to be anonymised or printed on request by a Data Subject either individually or in bulk.

Customer and Supplier accounts, including names and addresses, will be manually edited or removed when they are no longer required to be stored within Global 3000 (V6.0) in accordance with the business rules. Note that transaction data must be consolidated and cleared from the archives before account records can be physically deleted. Addresses that are not required for transaction history can be manually marked for anonymization, these are then physically anonymised when the current accounting period is closed.

Anonymization of contact details takes place in two stages, initially a contact is marked for anonymization (at this stage the contact can be restored and physical anonymization will not take place), then when the current accounting period is closed the contact is physically anonymised (and then cannot be restored).

When a contact is physically anonymised, sales and purchase orders (for the account the contact belongs to) are automatically updated to anonymise any personal data matching that on the contact. Physically anonymised contacts are deleted from the database each financial year end.

Transactions (General Ledger, Creditors Ledger, Debtors Ledger or Cash Manager etc.) will not be automatically updated to remove any personal details captured, such as customer/supplier names.

Summary of Features

This section outlines the additional features within Global 3000 (V6.0) that have been designed to assist with the consideration of a business GDPR compliance strategy. These may be utilised in conjunction with other fields and flags within the Global 3000 (V6.0) product and may form part of the internal procedures for the management of personal data.

As stated above, these new features are designed to assist with the considerations on the implementation of the overall GDPR compliance strategy for the business and are not in themselves a complete solution. If in doubt, suitable legal advice and guidance should be sought in respect of the obligations for the business under the regulations.

Data Protection (GDPR Status) Information

Data protection settings (GDPR status information) are manually recorded against customer and supplier contacts. This information indicates that the contact was received via a third party, has opted in (to data retention as specified in the company's data retention policy), that consent to share data with third parties has been provided, that consent for use of data for marketing purposes has been provided and an indicator that the contact has been made aware of the company's privacy notice. It also enables you to record when a contact opts out (of data retention) and when details have been shared with a third party.

In addition, the data protection settings enable a contact's details to be retained until a specific date. If this feature is used, this date is checked by close period (Debtors Ledger or Creditors Ledger) and if the start of the new period is later, the contact details are automatically anonymised.

Creation/amendment of a contacts data protection settings are included when account details are audited.

The data protection settings held for each contact are:

- Contact creation date.
- Contact details were received via a third party.
- Contact opted in to data retention (and the date they did so).
- Contact details are to be retained until a specific date (and the date).
- Contact opted out of data retention after having previously opted in (and the date they did so).
- Permission given to share details with third parties.
- Contact agreed to receive marketing material.
- Contact made aware of company privacy notice (and the date they were).
- Contact details have been shared with a third party (and the date they were).

Data Protection Maintenance (used for GDPR Control) – New Function

This new function (to which access can be limited to suitably authorised data controllers via an authorisation point) allows you to manage the data protection preferences for contacts (either individually or in bulk). It lists all contacts (either customer or supplier), the user will then locate the desired contacts and select them for further processing. Once all required contacts have been identified and selected the user can then update the data protection settings, anonymise the contacts, print the full contact details or record the fact that the contact details have been shared with a third party (including recording details about the third party).

Data Subject Access Requests (DSAR)

These can be processed by locating and selecting the contact within the data protection maintenance function. The 'Print' option can then be used to produce a PDF format document that can then be sent to the data subject.

Right to be forgotten/Opt out requests

If the data subject requests to opt out of data retention or invokes their right to be forgotten, locate the contact (either within account maintenance, enquiries or data protection maintenance), then update their data protection settings to record the fact that they have opted out of data retention. Then mark the contact for anonymization.

Marketing Material

When Global 3000 (V6.0) delivers documents via email (e.g. POP Orders, Invoices, Customer Statements, Remittance Advices etc.) the system can be configured to include up to five additional documents as attachments. These attachments have a new setting to indicate whether or not they are marketing material.

The recipient of the emailed document is checked against the contacts for the account, if it matches the email address for a contact that has not agreed to receive marketing material then attachments that are marked as being marketing material are not included.

Technical Details

The following address and contact data is currently held within Global-3000.

Name and Address table (Database PARAS table Addresses_PA)

Account name	Name
Address 1	Street
Address 2	Suburb
Address 3	State
Address 4	Country
Post code	Post_Code
Country	Country_Code
External account	External_Account

All the above details (with the exception of the country code) are cleared when an address is anonymised.

Name and Address table (Database PARAS table Contacts_PA)

Contact name	Contact_Name
Salutation	Salutation
Position	Contact_Position
Telephone	Telephone
Fax number	Fax_Number
Email address	Email_Address
Web address	Web_address
Mobile	Mobile_Phone_Number

All the above details are cleared when a contact is anonymised.

The following contact data (data protection settings) are held as an addition to the contact record (redefining Database PARAS table Frame_Parameters_PR). It is our intention is to merge these fields into the main contact record when the next version of the PARAS database is released.

Date contact created	Contact_Created_Date
Contact received via 3rd party	Created_Via_3rd_Party
Opted in to data retention	Data_Retention_In
Opted in by operator	Data_Retention_Opid
Date opted in to data retention	Data_Retention_Date
Time opted in to data retention	Data_Retention_Time
Retain details until date	Retain_Until_Date
Date to retain details until	Retain_Date
Opted out of data retention	Data_Retention_Out

Opted out by operator	Out_Data_Retention_Opid
Date opted out	Out_Data_Retention_Date
Time opted out	Out_Data_Retention_Time
Share details with 3rd parties	Ok_Share_3rd_Party
Agreed to receive marketing material	Marketing_Material
Aware of privacy notice	Privacy_Notice_Aware
Date aware of privacy notice	Date_Privacy_Notice
Time aware of privacy notice	Time_Privacy_Notice
Operator made aware of privacy notice	OPID_Privacy_Notice
Detail shared with 3rd party	Details_Shared
Date details last shared	Date_Details_Shared
Contact has been anonymised	Details_Anonymised
Anonymised by operator	OPID_Anonymised
Anonymization type	Anonymised_Type
Date anonymised	Date_Anonymised

The above details are deleted when the corresponding contact is deleted.

To aid resellers with their own vertical applications a new reseller intercept point has been added so that reseller software can detect when a contact is added, amended or deleted and when a contact is anonymised by close period.

In addition, the data protection settings for a contact are processed via a DLM routine that can be invoked by reseller software if required. Full details are available upon request.

Note: the details in this document are subject to change. Should you require any further information or assistance please contact your Global support provider.