Development Documentation

GDPR: Anonymisation of Customer/Supplier Information.
## Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>28/03/2018</td>
<td>Initial Release Version</td>
</tr>
<tr>
<td>1.2</td>
<td>04/04/2018</td>
<td>Update to outstanding debt functionality</td>
</tr>
<tr>
<td>1.3</td>
<td>16/05/2018</td>
<td>Update to changed functionality</td>
</tr>
</tbody>
</table>
Contents

1. Overview .......................................................................................................................... 4
2. Specification .................................................................................................................... 4
3. Configuration .................................................................................................................. 4
4. Usage .............................................................................................................................. 5
1. Overview
Khaos Control Solutions Ltd have developed Khaos Control to create new Anonymisation tools to support your compliance with the new GDPR legislation.

2. Specification
User Stories:

✓ As a business owner I want to ensure that Khaos Control allows me to easily meet my obligations under the EU data protection regulations (specifically the GDPR). My staff should be able to anonymise and hold data of customers who request it.

✓ As a sales/customer services operative, I want to be able to click a button to anonymise or hold a customer’s information, so that the customer’s right to anonymity and right to restrict processing can be protected if they request it.

GDPR goes live on 25th May 2018. This development should be put through User Acceptance Testing and implemented into the system prior to this date to ensure your team have the tools they need. These changes alone are not sufficient, they will need to be backed up by a comprehensive GDPR training program for your staff.

3. Configuration
Database Configuration has been done. KSCL have configured this, as part of applying the update.

016486: GDPR: Implement a method to anonymise customer/supplier information.
Further, customer-specific set up is possible. There are values within System Values and within the Admin Passwords in System Data which relate to this functionality.

[ System Values | Company | Anonymisation ]

1. Anonymisation Data. (Value to use when overwriting customer data; this value over-writes the database and is permanent.)

2. Minimum Days Since Last Order. (Cannot Anonymise a Company until this many days has passed since their last Sales Order; the user will be told this and will be provided with a Sales Order reference to inform the customer.)

3. Company item to anonymise. (Tick-box list of what should be anonymised.)

4. Address items to anonymise. (Tick-box list of what should be anonymised.)

5. Anonymisation Debt Handling. (Option to prevent or warn if Customer has outstanding debt above threshold below.) (The outstanding debt is amount owed and does not take into account unallocated payments.)

6. Anonymisation Debt Value. (0.00 is treated as £0.00, as expected.)
Please note: The system is automatically configured to anonymise the contact forename and surname and the address lines 1 and 2. This is not configurable.

An Admin Password can be set in [System Data | Admin Passwords] > Customer Anonymise. This will show as being set (a series of stars) whether a value has been entered or not.

Please note: Where this System Data password is not setup the functionality will work without requesting a password from the user.

016488: GDPR: Add a flag to prevent a user`s data from being processed.
The following System Values should be set:

System Values > Companies > Data Holding

1. Holding Data. (Label to visually overwrite data, the data integrity is maintained behind the scenes.)
2. Held Data is removed from hold by a new Sales Order. (Yes/No, controls if a new Sales Order will clear the `held` flag against the Customer.)
3. Held Data is removed from hold by a new Purchase Order. (Yes/No, controls if a new Purchase Order will clear the `held` flag against the Supplier.)

An Admin Password can be set in [System Data | Admin Passwords] > Customer Hold. This will show as being set (a series of stars) whether a value has been entered or not.

Please note: Where this System Data password is not setup the functionality will work without requesting a password from the user.

016535: GDPR: Make sure that webservice provided by Khaos Control Solutions are GDPR compliant.
An updated webservice is required.

4. Usage

016486: GDPR: Implement a method to anonymise customer/supplier information.
After applying the above Configuration, typical steps for usage would include:

1. Open the Company Record to Anonymise all or part of.
2. The Company record can be Anonymised (which will anonymise both the Contact and Address) by selecting `Anonymise Company` on [Customer | Detail | General].
3. An Address can be Anonymised from [Customer | Detail | Address] > Address section > Anonymise Address.
4. A Contact can be Anonymised again from [Customer | Detail | Address] > Contact section > Anonymise Contact
5. When performing these 3 the Company record, the User will be warned this process is not reversible. After which, the process is confirmed, with the warning prompt to look for further identifiable data; the appropriate data will have been anonymised.

Please note: with all Anonymisations, the User should check for other items which are associated and therefore may need anonymising, for example CRM entries, comments/complaints and Bank Details.
The User should also check for any other Company Records which pertain to the same Customer or Supplier.

![System Data Admin Passwords](image)

The System Data > Admin Password screen values you need to ensure are setup if you want to control how and when the anonymisation or hold-data functionality are to be used are:
- Customer Anonymise
- Customer Hold

The following System Values sections should be reviewed and setup as desired:
System Values > Companies > Anonymisation
System Values > Companies > Data Holding

IMPORTANT: If these passwords are not configured the system will not allow you to interact with the functionality they control. This is a safety measure to prevent systems from allowing mass-anonymisations without overseight.
Figure 4b: Anonymise Company and Mark Company as Held
Please note: if the User enters edit mode, Anonymises, then Cancels edit mode. Anonymisation is still done: Anonymisation does not require Edit mode.

Please note: if database back-ups are taken and kept then personal data will be stored in them. This will mean you could be in break if a customer requests to be anonymised and you have to restore to a previous backup point. Please ensure you are keeping regular backups and are only keeping the most recent to minimise your exposure to this risk.
Audit Log

The Audit Log will document Anonymisation changes and will also be anonymised when the process is run. A user can make use of the Document Kind filter see these changes. The audit filters can also help the user to find changes to the data protection related flags, alongside reasons for these changes.

The Audit Log can be reached from [ File ] menu at the top of Khaos Control (with appropriate permissions.)

016488: GDPR: Add a flag to prevent a user`s data from being processed.

Marking a Company as Held is done from the button next to Anonymise Company (see figure 4b above). This keeps the data of the Company record intact but will anonymise company data elsewhere in Khaos Control. These areas include [ Sales Orders | List ], [ CRM ], [ Sales Summary ] and [ Accounts ].

Note there is a System Value option which will control whether the held flag is re-set when a new Sales Order is raised. This is because making a new Sales Order may or may not give consent for data to be used again. Due to this ambiguity we have provided you with the ability to control how your system behaves and so be compliant within your understanding of the GDPR rules. The Option is [ System Values ] > Companies > Data Holding > ‘Held data is removed from hold by new Sales Orders’. Please note: there is a corresponding option for Purchase Orders.

Regardless of the state of the option mentioned above the customer’s data is not held from a Sales Order, as the order requires it to be pick/pack/despatched.

016535: GDPR: Make sure that webservices provided by Khaos Control Solutions are GDPR compliant.

The webservice will export the anonymised data (with the fields anonymised.) If the anonymisation is done at the Company record, the exported data will have <HIDE_COMPANY> set as ‘-1’, within the <Company> header. Likewise, there are <HIDE_ADDRESS> and <HIDE_CONTACT> tags within the <ADDRESS> and <CONTACT> headers respectively, if the anonymisation has been done at this level.

For a Held Company, data will be exported as normal. That is the data will be shown. Held will be exported with a <HOLD_DATA> flag set as ‘-1’. This will be exported at the each of the <COMPANY>, <ADDRESS> and <CONTACT> level.

The webservice calls that are affected include: ExportCompany; ExportOrders and GetCompanyInfo.
Notes / Caveats

Please note:

1. The Anonymisation process is not reversible. If the customer wants further products after they have been anonymised, then they will need to be allocated a new customer record.
2. Past Invoices are linked to customer records for their data, therefore Anonymised information will be anonymous on the invoice as well, along with other documents. The length of time the customer must wait before being anonymised should therefore be setup with care.
3. If you were to de-dupe on the fields Company Name / Address 1 etc, but you have Anonymised or Held the data, these will be highlighted for a merge.
4. Functionality has been extended to exclude Customers, or put additional checks in place, where the Customer has outstanding debt. These are controlled by System Values ‘Anonymisation Debt Handling’ and ‘Anonymisation Debt Value’, mentioned above. Otherwise [ Accounts | Debt Management ] would be anonymised. Please note this value
5. The EPOS customer should not be Anonymised. This is unlikely to be the case as there will be Sales Orders against this customer. If this is done, a new EPOS customer could be created.
6. Supplier Reference against a Stock Item is not Anonymised, the User should remove this, if it contains identifying information.
7. Only the first Order returned is shown in the information dialog detailing outstanding (current) Sales Orders.
8. The count in List Manager does not exclude Anonymised Contacts. A separate label shows above the grid as shown in Figure 4e below.
9. When Holding an Address / Contact on the customer form itself, the (held) state of the information is not shown. [ Customer | List ] will show the updated Invoice Address / Contact.
10. Anonymised and Held customers will have the identifiable portion of their email address anonymised. This is: [SV: Anonymisation Data]@KhaosControl.com and Hold@KhaosControl.com, respectively. The anonymisation email address is controlled by the System Value field, but the held email address has been hard coded as Hold@KhaosControl.com. Please avoid using an email addresses which might exist within your configuration, to avoid situations of sending or not sending where the opposite would be appropriate.

Email Subscriber / Mailing Flags

Email Subscriber and Mailing Flags are contained in the CONTACT table. They are named EMAILER_SUBSCRIBER and DATAPROT_ID. EMAILER_SUBSCRIBER is a Boolean and DATAPROT_ID is an ID. DATAPROT_ID can be cross referenced with the DATAPROT_TYPE table.

Please evaluate these for GDPR compliance.
Figure 4e: List Manager – Number of Anonymised Items label.