Corby+Fellas

WinRetail GDPR Program Update Notes (Release A)

17th April 2018

1. Introduction

The following notes describe the system changes to the Head Office, EPoS and Store Management modules of WinRetail that have been made to accommodate the requirements of the GDPR.

The notes refer only those programs that impact on the operation of the system and exclude those (the majority) that run behind the scenes and are invisible to the user.

2. EPoS and Back-Office Operation

About 120 programs have been modified to cope with the GDPR changes, 90% of which are relate to the storage and encryption of sensitive information held in the following database files, records and fields:

- Customer's Personally Identifiable |Information (PII)
- Customer Attributes, which hold additional information about customers, such as 'has pets', 'date of birth', 'opt-in' options, etc.
- Receipt Header record, which holds customer details that are captured during the processing of Sales, Returns and Sales Orders.
- Company Personnel details, i.e. all details of company employees, including: name, address, DoB, display names, operator initials, etc.

Every program that accesses customer or staff details must decrypt the details before they are displayed and/or processed and then re-encrypt them before writing data back to the database.

Customer Search

If a customer, who is a member of a loyalty or membership scheme, does not have their card or their card will not scan, their details must be found by using a search routine.

As customer details are now encrypted this means that the 'search customer' feature on the till can no longer easily search the database. The search now relies on an unencrypted table stored in memory, which is populated during the Tills Overnight process or, alternatively, when a user instigates the Customer Search process.

Real time changes (customer details that are changed at H.O, sent directly to the stores and updated as the till performs sales/transactions) are also updated in memory.

The decryption of every customer record is processor intensive and, in consequence, time consuming. We are expecting the decryption rate to be about 50,000 customer record/minute, hence the need to carry out the process at night.

Once the table is stored in memory it will stay in memory until WinPoS is exited.

The Search Customer program will no longer list multiple customers and their addresses.

To enhance system security the method of searching for a customer with no ID card has been changed as follows:

When a customer gives their surname, the system will indicate the number of matches as the name is entered, but no other information would be revealed. Having established their surname and assuming there was more than one person with that name, the customer will then be asked for their post code. In many cases this would produce a unique match; however, if this wasn't the case, they would be asked for their house number/name.

Once a unique match is found, the customer's details will be displayed.

The Right to be Forgotten

Those customers who wish to assert their right to be forgotten and to have their PII erased, will now have their database entries removed and their history masked/anonymised. A process at Head Office triggers the deletion event (see below).

Purge Routines at Till and Store Level

Customer's personal details will appear on Sales and Transaction History files, and on the till's Daily Journal files.

There are now purge routines at store and till level, that will automatically remove receipt and sales order transaction history after it has been stored for more than a pre-defined number of days (a user definable INI file setting, with a default value of 60 days).

In addition, Till Daily Journal files will be automatically deleted after a pre-defined number of days (also a user definable INI file setting, with a default value of xx days).

Till Journals

Till Journals now contain encrypted customers details as opposed to clear text. Journals are, as has been mentioned, regularly purged together with any other working directories.

Customer Sign-Up at a Till

Customer Sign Up and modification at the till now insists the relevant Opt In flags are set. Please note that we no longer warn of duplication, as this could cause an existing registered customer's PII to be inadvertently revealed.

3. Head Office Operations

Data Encryption

Personal data held at a central, Head Office server is, by default, not encrypted. However, it may be encrypted using Progress Software Corporation's OpenEdge Transparent Data Encryption (TDE) tool, which encrypts all the data held on a Progress database. This option requires the use of Progress's Advanced Enterprise version of Open Edge (OE) 11.7.

Registered & Un-registered Customers

It is necessary to distinguish between registered customers (i.e. member of a loyalty scheme, club, etc.) and un-registered customers, who have provided personal data needed just for the fulfilment of a Sales Order or when booking a ticket(s) for a Special Event.

<u>Registered Customers</u>

Registered customers will have submitted their details via four possible routes:

- Sign up form at Store (staff have then entered their details via Customer Maintenance)
- Sign up process at the till
- Sign up via the App
- Sign up via the Web Site*

*Some users are yet to modify their web site Sign Up pages

In all cases customers must have agreed to the terms of your Privacy Policy and selected their Opt-In choices regarding marketing preferences.

It is only registered customers for whom it is possible to maintain personal details, as they will have been assigned a customer number allowing their data to be accessed.

All changes and events are recorded, together with a list of documents (Xprint, PDF, txt) that have been written to the servers file system.

For registered customers, a new, multi-function program has been created to allow the following GDPR related processes to be carried out:

- Access Data
- Rectify Data
- Suspend Processing
- Erase Data

There are additional database fields to accommodate the customer's GDPR status.

There are additional scanning routines to warn users of 'dormant registered customers' and, if appropriate, suggest that their records be removed from the database.

A customer is considered dormant if:

1. They have not visited any store (or web site if relevant)
2. There has been no activity against their account for a pre-set number of months, determined by the user (definable at program level).

Opt-In Replaces Opt-Out

Now that the GDPR requires that customers positively affirm their wish to Opt-In to any marketing activity, etc., we are retiring Opt-Out fields.

A 'one-off' conversion program, run from Head Office, has been created to set the status of these new fields; for example, the Opt-In option to receive marketing information via Post is automatically set to YES if the old Opt-Out option is set to NO. The reverse will happen if the old Opt-Out option is set to YES.

This 'one off' routine also allows users to default the new Opt-In option regarding the collection of 'Buying Information' (for Data Profiling) to YES. This assumes that most users will elect to default this to YES as customers will, by implication, have agreed to their data being captured and/or will have subscribed to Data Profiling at some point in the past.

For those users who want to ask their registered customers to confirm their agreement a new Customer Attribute has been created, labelled 'Reaffirm Opt In' which triggers a till message, prompting the operator to ask the customer to reconfirm their wishes regarding the receipt of marketing information via e-mail, post and/or SMS message, and if they wish to allow/disallow the collection of their purchasing data and/or allow/disallow their data being passed on to a third party.

Please note that the reaffirm options is not yet available via user's web sites.

<u>Un-Registered Customers</u>

In addition to the registered customers, who have signed up to the membership of a club, loyalty card scheme, etc., there are unregistered customers, whose personal data is required to be held, temporarily, when they:

- Place a sales order that requires delivery.
- Book an event via the Events Booking module
- Buy a stock item that has its 'Ask Customer's Name & Address" option set to YES.

.

These customers are only usually asked for their:

- Full Name *
- Postal Address including posts code
- Telephone/mobile number *
- Email address

*Usually mandatory

Details are recorded and encrypted at the Store so that customer's transaction can be processed and recalled; they are not asked if they wish to Opt-In to any marketing options, or to give their date of birth or any other personal information.

Furthermore, their details will not be used for CRM or data analysis purposes and they will not be exposed to marketing or other forms of analysis (e.g. geographic sales/coupon redemption). Any communication with them will only relate to their Sales Order/transaction (e.g. order ready for collection/delivery) etc.

We have now a purge routine that will mask non-registered customer details within a pre-set number of days after the completion of their transaction (e.g. full delivery of order). The back office and tills will also carry out a self-purging process for these non-registered customers.

They 'the right to be forgotten' cannot be applied to non-registered customers as:

- Unlike registered customers they do not have a unique customer number
- We can't rely on using their name (e.g. Mr Smith is likely to appear frequently)
- It is permitted by the GDPR for the information for processing if it is required for the business function
- The GDPR permits PII to be held and used for the completion of the retailer's legal obligations (see X days above).

Customer GDPR Options Program

A new multi-function program (see screen layout above) has been created to cater for the customer's data requests. It will be placed within the Head Office WinRetail menus under the Customer sub menu.

It should only be accessible by trained staff and those with sufficiently high access rights.

The program, which is designed to deal with one customer at a time, will not allow any processes to be carried out until the customer identity has been confirmed. In addition, the identity of the user accessing the program will be recorded.

We have not yet provided a Web page option (self-service) to enable to users to view, edit download or erase their personal data; although this will be available in the future.

If a Data Request is printed, the XPR output file will be immediately removed from the server following the completion of printing and the event will be recorded within the 'Customer Events' database table.

The Data Request option allow all captured information to be viewed (a list of Customer Attributes is optional), together with a summary of the customers Sales/Returns transactions. However, this will not include discounts, coupons redeemed, payment methods and loyalty points. In addition, we do not include CRM segments, mailing lists, open rate statistics, spend analysis or 'change' events (such as name/address changes).

A request for Erasure starts a chain of events, as follows:

1. A customer attribute record is created named 'Asked to be forgotten', which is transmitted to all stores, web servers and tableau servers.
2. An overnight Appserver Global Delete routine will spot this record and will flag the customer record for deletion
3. Each store, web site and Tableau server will recognise the delete flag and will remove the customers details from the database, together with their associated attributes
4. All transactional information containing their name address, such as Sales Orders, will be masked/anonymised (all sites & Tableau)
5. After a period of 6 days all database records associated with the 'erased' customer will be removed from the Head Office (they will have been removed at other locations within 24 hours). These include the following database tables:
    - Customer
    - Customer-event
    - Customer-card
    - Customer-document
6. Any customers details, which had been written to associated transaction files (receipts, despatches and sales orders), will be masked/anonymised
7. The customer number (and only the customer number) is written to a separate log to indicate that all data associated with that number has been erased. This log will be utilised in the event of a system backup being restored to ensure that any restored 'erased 'data is subsequently deleted (these customer numbers would have to be manually flagged for removal based on the backup date).
8. It is possible that the customer may receive direct mail, SMS or email during the 6-day processing period as these may have been generated before/within 24 hours of the rquest for erasure having been raised.

An 'erased' customer's record will no longer be detectable within searches and their transactional information will be masked.

4. Suggestions

At Head Office we suggest that the following routines should either have their menu permissions mad more stringent or become part of a User Group, as they allow customers details to be viewed (albeit, for the most part, just customer number and name):

- Customer maintenance
- Membership maintenance
- Import Customer Details
- Spring Marketing Campaign mailing list
- Mailing List Maintenance
- Campaign maintenance
- Segmentation Maintenance
- CRM Advanced (all menu options)
- CRM Utility (all menu options)
- Campaign Coupon Enquiry
- Customer GDPR Options
- Gift Card Enquiry
- Gift Card Status
- Till Sales Enquiry (H.O and B.O)
- Sales Order
- Sales Order Enquiry
- Print Account Invoices
- Print Sales Invoices
- Sales Order Despatch Notes
- Sales Order Inactivity
- Sales Order Enquiry
- Sales Order Margins Enquiry
- Sales Orders – Reserve and Put Away
- Management Purchases (staff purchases)
- Refund Ticket Enquiry
- EFTPoS Enquiry
- Picking Lists
- Sales Order Payment
- Sales Order Pick Schedule
- Stock Reservation Reminders
- Sales Order Warehouse Availability
- Price Band Maintenance (customer specific pricing)
- Customer Enquiry