rms
operational excellence

connect without compromise
metro

Retail Manager Solutions Limited

GDPR Products Statement

January 11th 2018

Retail Manager Solutions Ltd GDPR Statement

DOCUMENT CONTROL			
Version	**Author**	**Date**	**Summary of Changes**
1.0	RMS	11/01	Initial Publication
2.0	RMS	20/02	Amendments
3.0	RMS	26/02	Amendments

Contents

1. Overview

The purpose of this document is to give an overview of how the software products of Retail Manager Solutions Limited (RMS) will assist customers with their compliance with the GDPR.

Release versions as recommended by RMS for GDPR compliancy will be a prerequisite to RMS accepting its joint data processor liability under the new regulations.

The document will cover the 8 rights of the individual within the act and how the products will aid with compliance in these areas.

This document will also provide examples of personal and sensitive data that RMS may hold within standard fields in the system.

Wherever possible RMS will provide the full ability for the client to self-service the amending, retrieval or removal of data as required by GDPR.

Within this document we will refer to the 'client' as being any person associated or an authenticated physical user of the RMS solutions.

A major point that should be made is that GDPR and security compliancy is a shared responsibility between RMS and the clients.

2. Personal and Sensitive Data – Statutory Definitions

Examples of personal data

Names	
Addresses	
Date of Birth	
National Insurance Number	
Gender	
Next-of-kin details	
Image	E.g. digitalised photo of the user
Warnings	
Notes/Comments	Ad-hoc personal comments that may be entered
Forms	Customers need to consider non-standard fields stored in Forms created/customised by the client
Extra Client Fields	Customers need to consider sensitive data that may be stored in Extra Data fields created/customised by the client

Examples of Sensitive Data

Ethnic Origin	
Sexuality	
Religion	
Bank Account details	
Medical details	Communication preferences, impairments etc
Criminal history	
Social Work	
Eligibility to work details	
Notes/Comments	Ad-hoc personal comments that may be entered
Forms	Customers need to consider non-standard fields stored in Forms created/customised by the client
Extra Client Fields	Customers need to consider sensitive data that may be stored in Extra Data fields created/customised by the client

Customers Data Controller Statement should say why the data is captured, what the purpose is for and how long it is retained. This is to comply with the parts of the regulations that state that data is collected lawfully, fairly and in a transparent manner. In reality, this will require each customer to perform a privacy impact assessment on personal and sensitive data that it collects and processes. There is guidance on the ICO website regarding performing privacy impact assessments. The statement must also show how the data is kept up to date and is accurate and is only held for the period where it is relevant. How the data is stored, secured and monitored for unauthorised access should also be detailed.

For personal data, the following legal gateways are valid.

- Consent
- Necessary in relation to the processing of a contract
- Legal obligation
- Vital interest – a matter of life and death
- Justice, Government, Statutory
- Legitimate interest

For sensitive data, the following are also valid.

- Consent
- Employment law
- Vital interest
- Legal proceedings, Legal advice or defending legal rights
- Administering justice
- Medical Reasons
- Equal opportunity monitoring with safeguards
- Crime prevention / malpractice

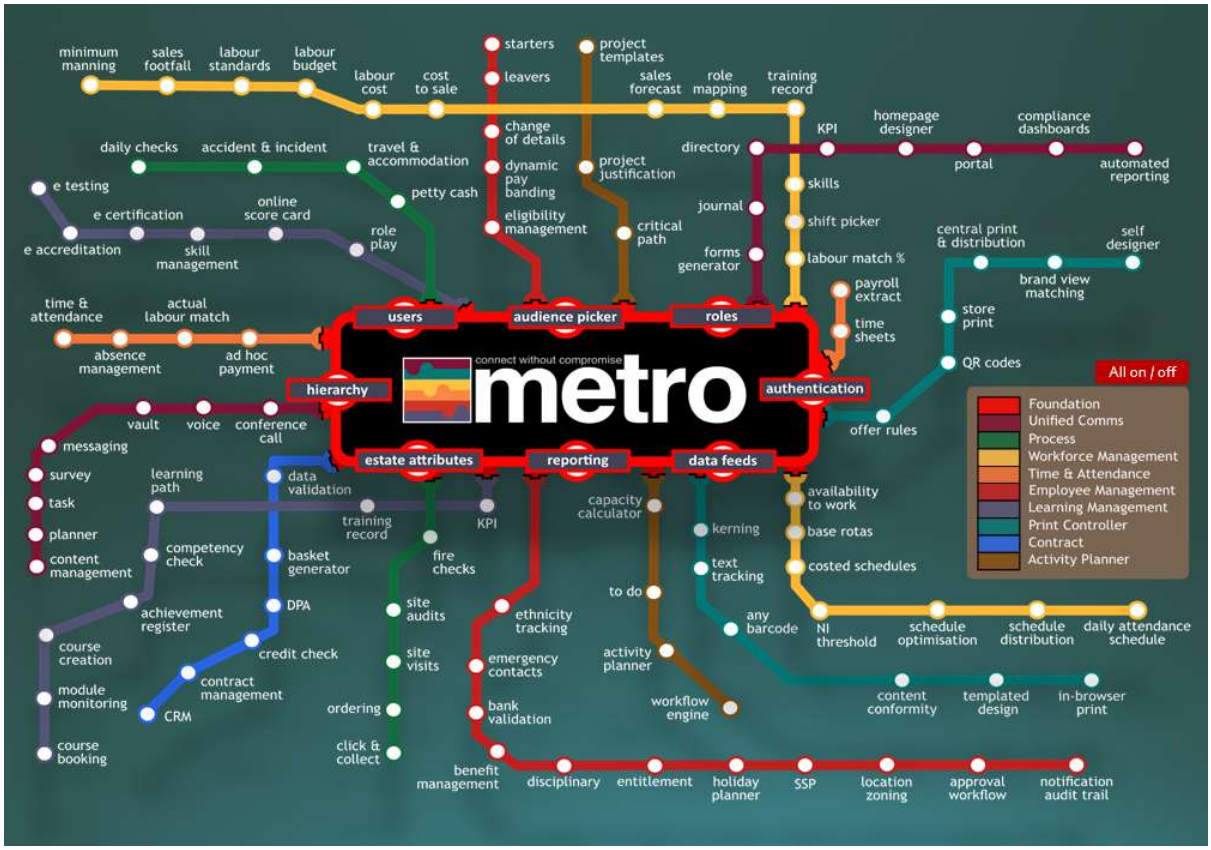
3. The Eight Rights of The Act

3.1 The Right to Be Informed

As a Data Controller, you should inform the client of the types of data that you are capturing, why you are capturing it and how long it is retained. It is also necessary to inform the client regarding how data is shared with other systems and why.

RMS Products and Services

- Metro comprising the following:



3.2 The Right to Access

To comply with the Subject Access Request element of the regulations RMS will provide the client with full access to the client's data through the solution. This may be as an individual self-service portal as a standard, or requested through the client's internal support mechanisms. The RMS solutions have the ability for the customer to individually/group authorise the various areas of their solutions depending on their requirements. Where the customer utilises central operations to provide the function to clients, then the customer should create a Subject Access Report as a contact management record against the client with a defined set of actions and outcomes that allow reporting on the requests and their status. If self-service does not meet any of the requirements for the right to access for the client for any reason, then a Subject Access Request (SAR) will be able to be raised on the RMS support system by the customer's authorised personnel, for actioning by RMS.

3.3 The Right to Erasure

Following on from a Subject Access Report a client may request all or partial erasure of data. The erasure request should be created as a contact management record against an individual with a defined set of actions and outcomes that allow reporting on the requests and their status. It is suggested that a before and after Subject Access Report are provided as proof of the removal along with a confirmation letter stating the outcome of the process. If self-service does not meet any of the requirements for the right to erasure for the client for any reason, then a Subject Access Erasure (SAE) will be able to be raised on the RMS support system by the customer's authorised personnel, for actioning by RMS.

3.4 The Right to Rectification

Following on from a Subject Access Report a client may request all or partial rectification of data. The rectification request should be created as a contact management record against the client with a defined set of actions and outcomes that allow reporting on the requests and their status. It is suggested that a before and after Subject Access Report are provided as proof of the rectification along with a confirmation letter stating the outcome of the process. If self-service does not meet any of the requirements for the right to rectification for the client for any reason, then a Subject Access Rectification (SARE) will be able to be raised on the RMS support system by the customer's authorised personnel, for actioning by RMS.

3.5 The Right to Object

Following on from a Subject Access Report a client may object to certain aspects of processing. The request should be created as a contact management record against the individual with a defined set of actions and outcomes that allow reporting on the requests and their status.

It is suggested that the individual is sent a confirmation letter stating the outcome of the process.

3.6 The Right to Restrict Processing

Following on from a Subject Access Report a client may object to certain aspects of processing. The request should be created as a contact management record against the individual with a defined set of actions and outcomes that allow reporting on the requests and their status.

It is suggested that the individual is sent a confirmation letter stating the outcome of the process.

3.7 The Right to Portability

A client may request an export of their data in a recognisable format. The request should be created as a contact management record against the client with a defined set of actions and outcomes that allow reporting on the requests and their status. It is suggested an export is provided of the data along with a confirmation letter stating the outcome of the process. If the client has requested erasure of their data then a confirmation certificate should also be provided. If self-service does not meet any of the requirements for the right to portability for the client for any reason, then a Subject Access Portability (SAP) will be able to be raised on the RMS support system by the customer's authorised personnel, for actioning by RMS.

3.8 The Right to Manual Processing

Following on from a Subject Access Report a client may request manual intervention in a process. The request should be created as a contact management record against the client with a defined set of actions and outcomes that allow reporting on the requests and their status.

It is suggested that the client is provided with a confirmation letter stating the outcome of the process.

4. How the data is retained and removed

This section relates to the data minimisation by implementing a retention policy on key records and fields.

The aim of Data Archiving is to aid compliance with the Data Retention Polices as set out in the regulations.

Minimisation of all data accessible to users is provided as a facility (based on individual or group authorisation) to all customers; it is the responsibility of the customer to inform RMS when permanent or hard deletion of inaccessible data is further required.

RMS operates a 30-day data backup retention period only.

5. Consent Management

A new section of a client's personal records should be introduced where consent for processing can be managed. This will require new fields that describe the type of usage of the data, the type of data being processed, the legal gateway being used to justify the usage and the start and end period of the consent. Where restrictions or objections to processing are deemed appropriate to interfaces then the consent records should be checked to prevent export of any said data.

RMS will assume that if a client is provided by the customer with an authorised user logon details, that the client has provided consent to the usage and any data processing with the RMS solutions.

6. How the Data is Secured

The RMS Metro implements the best practice with a layered and organised structure to provide Privacy by Design.

The RMS Solutions and environments will provide for the best security and availability practices including dual data-centre usage as a minimum to ensure constant availability of access to data; Firewalling controls; Anti-Virus/Malware services; IPS/IDS servicing; 24-hour systems' monitoring and alerting functions; obfuscation/encryption of any sensitive data; encryption of all traffic between systems, including to the client's system; encryption at rest; authentication options for password controls and complexity; authorisation levels with no access by default and least required level access provision. In addition, RMS support personnel follow security training, policies and procedures, and additionally will not have direct access to view or extract client sensitive data direct from data sources.

7. Prerequisites

Software Versions applicable:

All versions of Unified Comms from version 1.0;

All versions of Operations Director and People from version 4.0;

Active RMS support/helpdesk services contract in-situ.

Other Recommendations from Retail Manager Solutions:

Review of Metro access granted to staff/work groups.

Microsoft security updates are implemented on all machines.

Device security updates are implemented.

Anti-virus and malware software is implemented and up to date.

Device management software for mobile devices are implemented and up to date.

Customer should review any third-party software that they directly contract to. Within the current RMS Solutions, specific customers utilise such as Bank or Address Validation software and Yapster.

RMS direct Partners:

GDPR statements and policies can be found for the partners RMS utilises for the Metro solutions at:

Microsoft (infrastructure/software): https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx

AWS (infrastructure): https://aws.amazon.com/compliance/gdpr-center/

Twilio (discussion/conferencing): https://www.twilio.com/gdpr

SendGrid (mailing service): https://sendgrid.com/policies/tos/

8. Summary

RMS products will implement the following items of the act in the ways described in the individual sections which in summary are,

- The 8 rights of the individual in the act will be managed through by the customer and where applicable RMS, actions and outcomes with the ability of RMS support. Specific actions will need to be taken dependent on the rights being invoked.
- As part of the Metro platform RMS will provide a tick box to implied consent as part of the first log on access to the system and for password reset screen. This includes a renewal automatic at first logon and customisable customer privacy statement. If the authenticated user does not tick the box then the client will not be able to access the system. An exportable log will be made available for all password changes/renewals.
- Privacy by design is implemented by the current Metro functions audit, encryption and redaction functions and workgroup functions in Metro
- Data minimisation is implemented by the current Metro functions and specific retention policies.
- Other recommendations regarding general security requirements.

Further reading:

UK Information Commissioner's Office(ICO): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

EU Commission: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN