This is not intended to be legal advice

GDPR

Explanation of new functionality

Index

Document control				
Security level	Public			
Company	Amadeus IT Group SA			
Department	R&D			
Author	Chantal Ribbink			
Reviewed by	CR		Date	18-04-2018
Approved by			Date	
Version	Date	Change	Comment	By
1.0	05-04-2018	Creation		CR
1.1	09-04-2018	Adjustment of prntscrn.	Preferences	CR
1.2	10-04-2018	Addition	Purge	CR
1.3	12-04-2018	Addition	Preferences	CR
1.4	18-04-2018	Addition	Introduction	CR

Introduction

PMpro Version 10.02.143.XXXX will enable you to apply GDPR rules. Please be aware that this version does not automatically make your hotel GDPR compliant. The hotels will be responsible for setting up policies and procedures to ensure GDPR compliance and will also be responsible for the correct use of the system.

In this document the new functionalities will be explained.

Please make sure that you read the entire document and especially the part about the mandatory manual contact purge on page 7. This needs to be completed as soon as you receive the update in order activate the automatic purge during night.
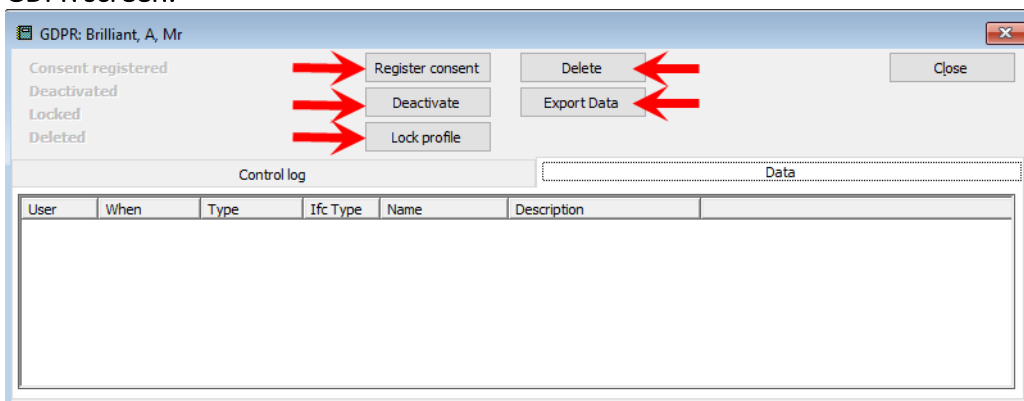
Manage contact profiles

A new button was added to the contact query screen. The button 'GDPR' will give a user access to the GDPR options.

Contact query screen:
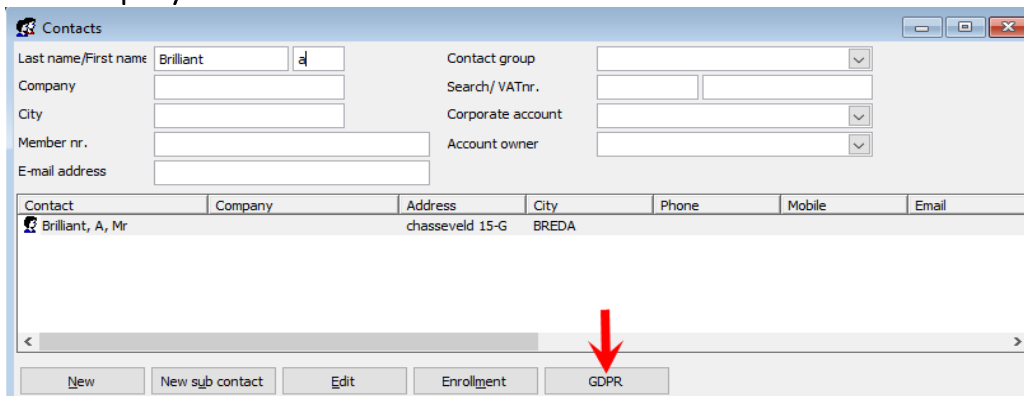
GDPR screen:

Save consent / Revoke consent

After a guest has given consent you can click on the button 'Save consent'. There are two options. Consent may be in writing or oral form.

1. Verbal consent

You can select this option if the guest answered 'yes' to a clear oral consent request. Please keep in mind that it can be difficult to prove oral consent and therefore using a consent document is advisable.

2. Document

You can select this option if the guest has signed a consent statement on a paper form. Please click on the three dots and select the location where you have stored the file that was used to register the consent. This can only be saved outside of in the PMpro directory, for example on a shared network drive. The location of the consent form will be logged in the control log. The hotels are responsible for the backup of the consent document.
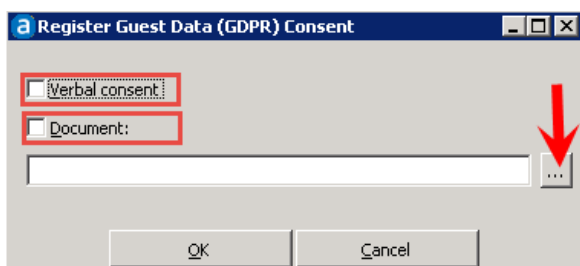
When you click on Save Consent the button will change to 'Revoke Consent'. You can click on Revoke consent to cancel the consent. Contact profiles with consent will not be purged.

Deactivate / Activate

Individuals have the right to 'restriction of processing' of their personal data. If a guest wants to have his profile deleted, but it cannot be deleted yet (for example because of the retention policy for invoices) you can deactivate the contact profile. It will become greyed out and you cannot select it on any new reservations. If you try to select a deactivated contact on a new reservation you will get the following message:
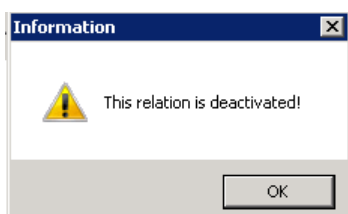
When you click on 'Deactivate' the button will change to 'Activate', so you can change the contact profile back to active when the dispute is resolved.

Lock / Unlock

When you lock a contact profile it will become locked for editing (all details will be greyed out), so nothing in the profile can be added, removed or changed. When you click on 'Lock contact' the button will change to 'Unlock', so you can unlock the profile when needed. Locked profiles will not be purged. In case of a dispute (for example about accuracy of the personal data or if the processing is unlawful but the guest objects to erasure) you can lock the contact profile until the dispute is resolved.

Delete

When you delete a contact it will be removed. Only the address ID number will be saved. In the GDPR preference settings you have to define a minimum amount of days before a contact can be manually deleted. This will be further explained in the chapter 'Preference Settings'.

Export data

Option to export contact data log in XML format. When you click on 'Export Data' you can select a location to save the file.

Control log and Data log

The control log can be used by the hotel to track what was done with a contact profile. When you use any of the above mentioned GDPR options this will be logged in the control log.

The data log contains information for the guest. It contains information about reservations, and it will show when guest data was used for reports, export and when guest data was send to an interface (for example CRS or telephone system).

User rights

Several new user rights are added in order to manage which users have access to the new GDPR options. All user rights are disabled by default and need to be activated by a manager.

You can go to setup>users>user rights and then select the user group.
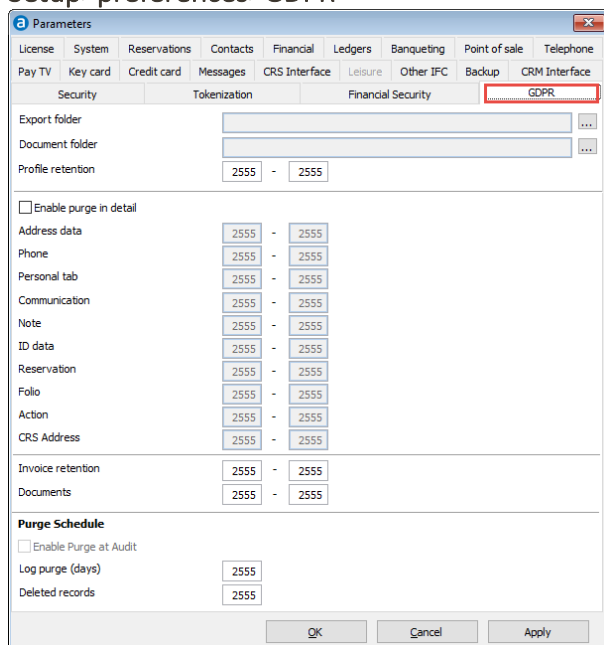
Under 'Setup/contacts' you can activate the right to manage the GDPR System Preferences and under 'Contacts' you can activate the rights to manage a contact profile (GDPR button) and for each GDPR function a separate right can be activated.

User rights screens:
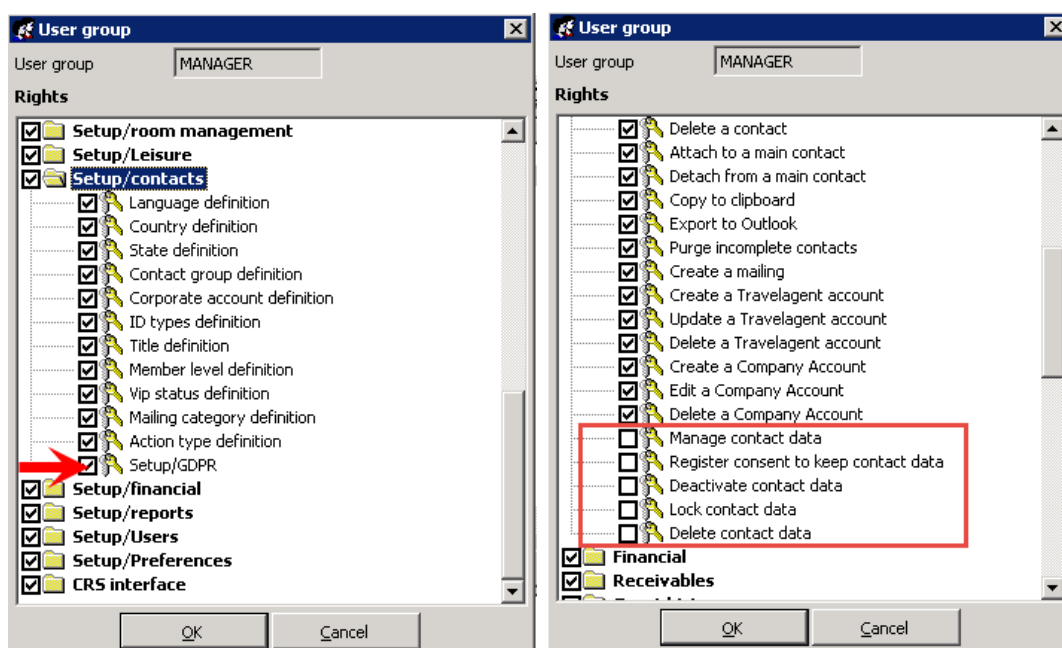
Preference settings

Setup>preferences>GDPR

Export folder: Default location to save the XML export of contact profiles.
Document folder: Default location for consent forms.
** These default locations need to be a shared network path which should be accessible from all workstations.

Profile retention: The minimum and maximum amount of days a contact profile needs to be saved after check out. Once the minimum amount of days have passed you are able to manually delete the contact profile. When you reach the maximum amount of days the contact profile will be removed during the automatic contact purge.

Enable purge in detail: Ability to set a retention policy per data group.

Invoice retention: The minimum and maximum amount of days a contact profile needs to be saved when used on an invoice.

Documents: The minimum and maximum amount of days documents are saved in the PMS/documents folder.

Enable purge at audit: If you activate this option, the contact purge will be done automatically during night audit.

**Log purge (days):** Number of days the IFC log files are saved.

Deleted records: Number of days deleted records are saved. When you delete data in PMpro and run a database maintenance, this data will be removed from the PMS and moved to the PMS/Packed folder.

Manual contact purge

After the update it is mandatory to do a one-time manual contact purge to clean up your address database. Before you start the manual contact purge you have to go to setup>preferences>GDPR and review all retention policies and make adjustments where needed. By default all retention policies are set to 2555 (7 years). If you want to use the detailed purge then tick the box 'enable purge in detail'. Now enter a minimum and maximum amount of days for each contact data category and click 'ok' to save this.

To start the manual purge you can go to Tools>Purge Contacts. The first contact purge can take several hours to complete, depending on the size of your address database. This manual purge can be stopped by clicking on the 'escape' button on your keyboard. You can start it again by going to tools> purge contacts. It will continue where it previously stopped. Once the manual contact purge is completed the automatic contact purge in night audit will be enabled in the GDPR preference settings. After the manual purge it is mandatory to run a full database maintenance. Tools>database maintenance> tick all 4 boxes > start. This needs to be completed before you run the night audit.
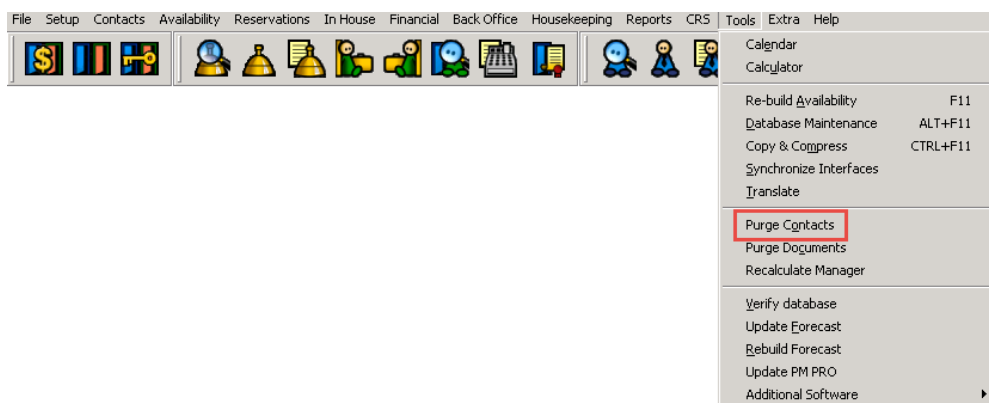
GDPR report

Under reports>contacts a new report is added: _GDPR change log
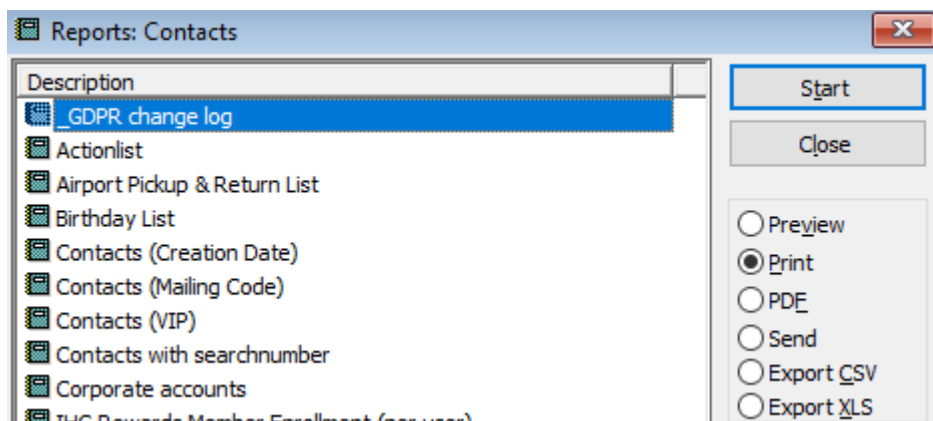
This report shows which GDPR options were used for contact profiles.

You can run this report for a date range and possibility to filter on:

- **User**
- **Address ID**; when you delete a contact only the address ID will be saved. When you look up an old reservation and you see that the contact profile is deleted you can copy the address ID in this report to see when it was deleted and by which user.