AZOTEL S10-02 v003 (2017-12)

S10 - Azotel GDPR Documentation

Azotel Technologies Ltd,
3rd Floor, River House,
Blackpool Park,
Cork,
Republic of Ireland.

Azotel Canada Inc.
325 Vulcan Avenue
NS B1P 5X1
Sydney
Canada

Azotel Poland
PLAC Powstancow
Slaskich 17A/222
53-329
Wroclaw
Poland

Phone (EMEA): +353-21-234-8100
Phone (North America): +1-312-239-0680 / +1-902-539-2665
Phone (Poland): +48-71-710-1530
Phone (UK): +44-20-719-3417
Phone (South Africa): +27-11-083-6900
Fax: +353-21-467-1699
info@azotel.com

Contents

1. Introduction

The purpose of this document is to document the GDPR related features that have been developed and added to the SIMPLer platform.

2. GDPR Overview

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directives 95 / 46 / EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

GDPR was approved by the EU parliament on 14 April 2016 and will be enforced from **25 May 2018.**

2.1 Key Terms

Personal Data: Any information related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Data Processor: A processor is the entity that processes personal data on behalf of the controller.

Data Controller: A controller is the entity that determines the purposes, conditions and means of the processing of personal data.

2.2 Summary of Key Changes

The key changes in relation to GDPR are 4oncernin in table 2.2-1.

Key Change	**Description**
Increased Territorial Scope (extra-territorial applicability)	Applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. The directive will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not.
Penalties	Orgnanizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater).
Consent	Companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily 4oncerning form, with the purpose for data processing attached to that consent. Consent must also be easy to withdraw.
Breach Notification	Breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of

	individuals”. Breach notification must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, “without any undue delay” after first becoming aware of a data breach. The guidance for data breach is located here: https://www.dataprotection.ie/docs/EN/Data-Breach-Handling/m/901.htm
Right to Access	There is a right for data subjects to obtain from the data controller confirmation as to whether or not personal data 5oncerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.
Right to be Forgotten	Entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.
Data Portability	The right for a data subject to receive the personal data concerning them, which they have previously provided in a ‘commonly use and machine readable format’ and have the right to transmit that data to another controller.
Privacy by Design	Calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.
Data Protection Officers	There will now be internal record keeping requirements, and Data Protection Officer appointment will only be mandatory for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale of special categories of data or data relating to criminal convictions and offences.

Table 2.2-1: Key Changes

3. Azotel GDPR Features

The purpose of this section is to document the steps to enable and manage any GDPR related features in the SIMPLer system.

3.1 Subject Access Request

The process for Subject Access Request (SAR) has been streamlined in SIMPLer.

Based on the GDPR requirements, there is a right for data subjects to obtain from the data controller confirmation as to whether data concerning them is being processed, where and for what purpose. The controller also must provide a copy of the personal data free of charge and in an electronic format.

A new section has been added to the customer record in SIMPLer on the left-hand side of the customer record. The new section is called "GDPR" and shown in Fig. 3.1-1. The relevant menu for the SAR updates is called "Subject Access Request" and circled in Fig. 3.1-1.

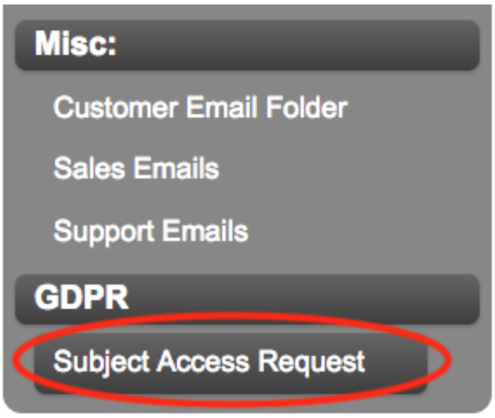
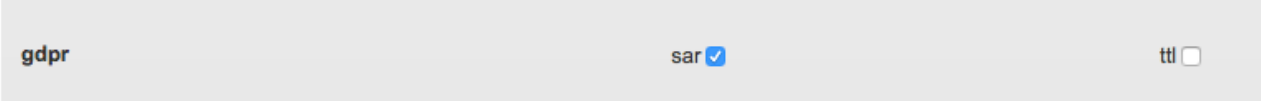


Fig. 3.1-1: GDPR: Subject Access Request

This section is driven by user rights on the user account. The section related to GDPR rights is called "gdpr" and the specific access right to use the Subject Access Request section is called "sar".

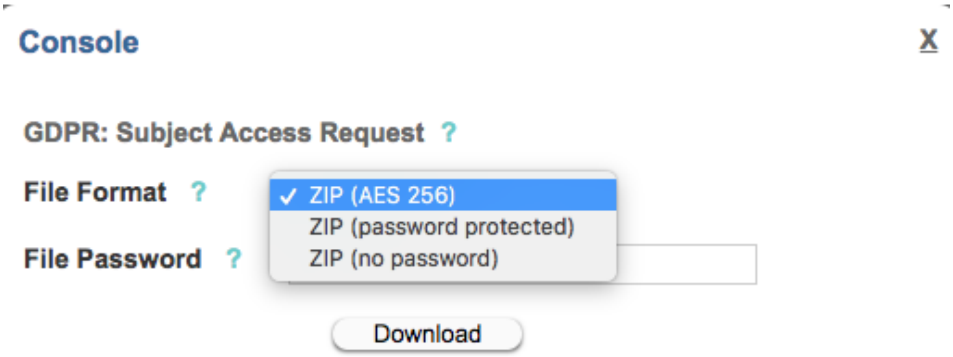


gdpr sar ☑ ttl □

Fig. 3.1-2: GDPR: Subject Access Request User Rights

By clicking on the "Subject Access Request" button shown in Fig. 3.1-2, the user can reach a console. This console presents several options to allow users to decide how data should be downloaded.

- ZIP (AES 256): AES 256 ZIP file with an automatically generated password required to open the files.
- ZIP (password protected): Standard ZIP file with an automatically generated password required to open the files.
- ZIP (no password): Standard ZIP file with no password required to open the files.



Console

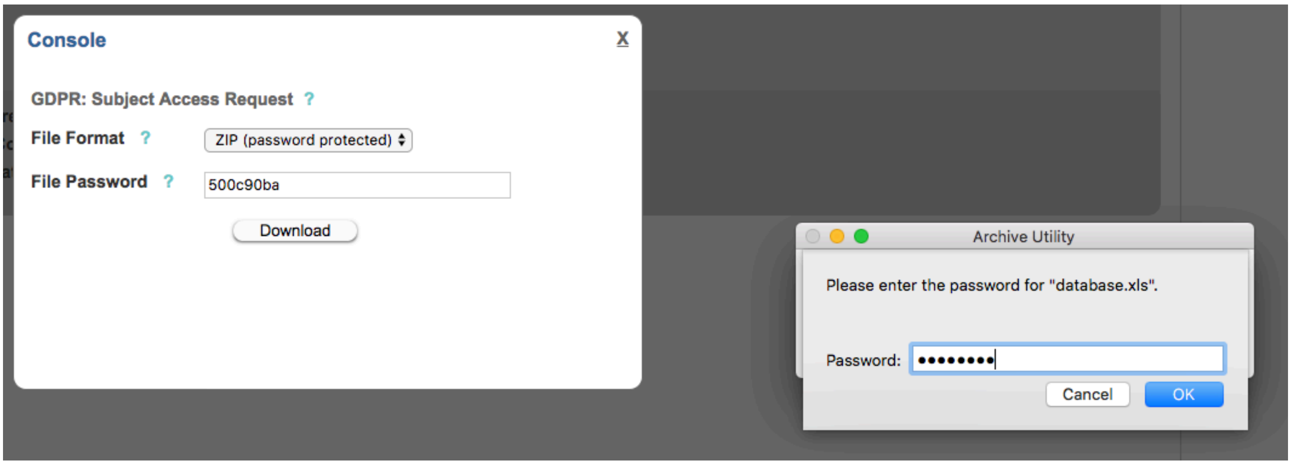
GDPR: Subject Access Request ?

File Format ? ✓ ZIP (AES 256)

File Password ?

Fig. 3.1-3: GDPR: Subject Access Request Console

Select the desired format from the drop-down menu shown in Fig. 3.1-3, for example "ZIP (password protected). Click download.
The ZIP files will download. For some options such as ZIP (AES 256) and ZIP (password protected), you will need to enter the password previously generated in the console to access them.



Console

GDPR: Subject Access Request ?

File Format ? ZIP (password protected)

File Password ? 500c90ba

Archive Utility

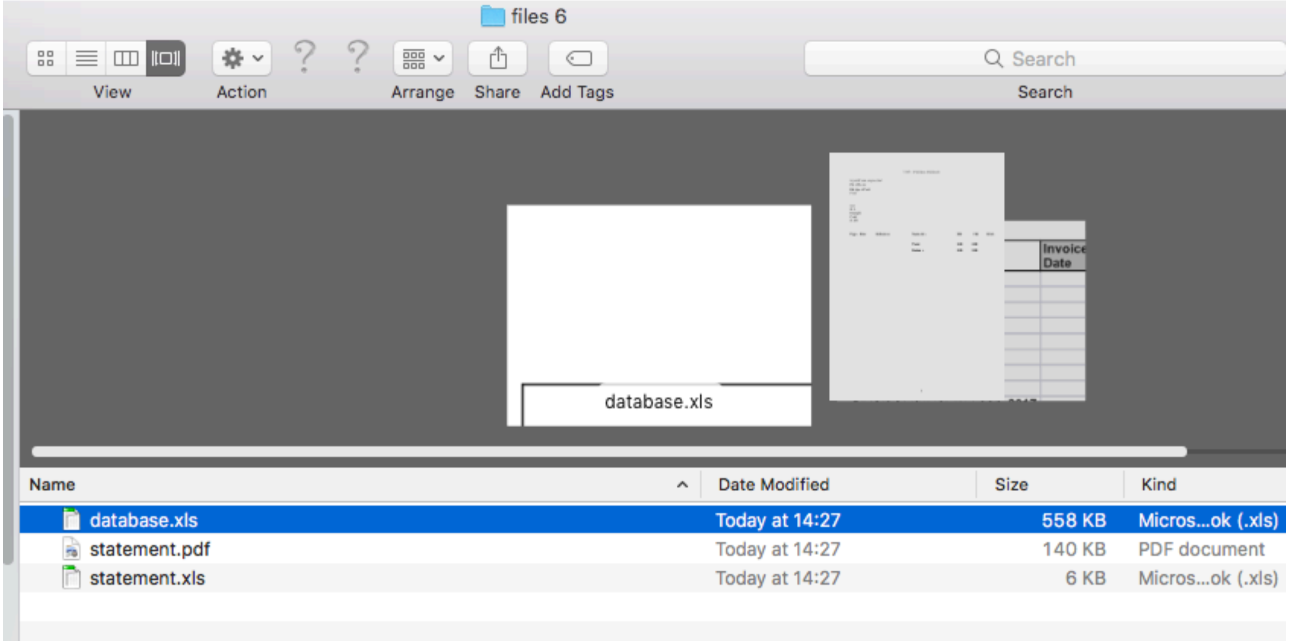
Please enter the password for "database.xls".

Password: ••••••••

Fig. 3.1-4: SAR download example password

The files downloaded will show:

- Database files: All stored details on the customer record. A tabbed XLS file containing basic customer details, billing details, subscriptions, sales details, tickets and all other relevant details.
- Statements: Customer financial statements in both PDF and XLS version.
- Attachments: Any attached files, photos, PDFs, etc.
- Invoices: All invoice PDFs.



Name	Date Modified	Size	Kind
database.xls	Today at 14:27	558 KB	Micros...ok (.xls)
statement.pdf	Today at 14:27	140 KB	PDF document
statement.xls	Today at 14:27	6 KB	Micros...ok (.xls)

Fig. 3.1-5: SAR download example files

The operator can send the data to the customer electronically, or redact the files before sending if necessary.

3.2 Time to Live

A new section has been added to the Settings Tab in SIMPLer. The new section is called “GDPR” as shown in Fig. 3.2-1.

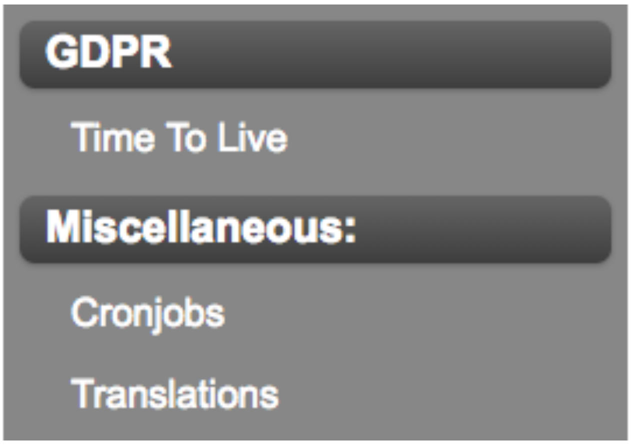
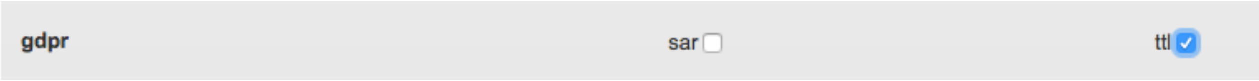


Fig. 3.2-1: Settings Tab – GDPR Section

This section is driven by user rights on the user account. The section related to GDPR rights is called “gdpr” and the specific access right to use the Time to Live section is called “ttl”.



gdpr sar □ ttl ☑

Fig. 3.2-2: GDPR: Time to Live User Rights

By clicking on the “Time to Live” button shown in Fig. 3.2-3 the user can access the Time to Live Settings page.

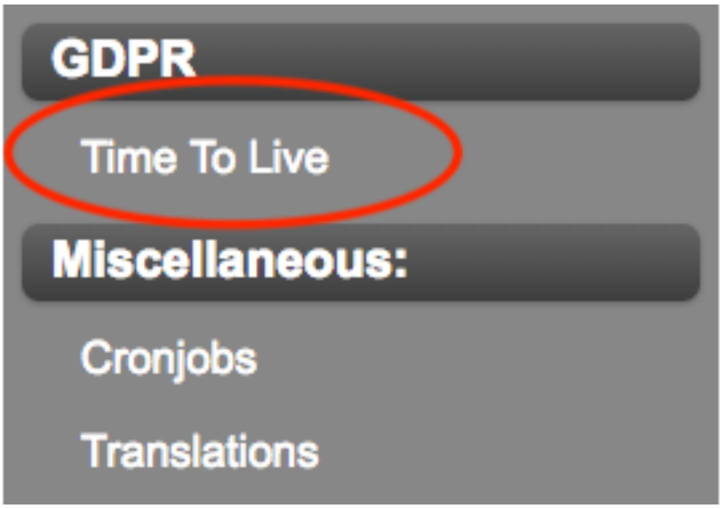
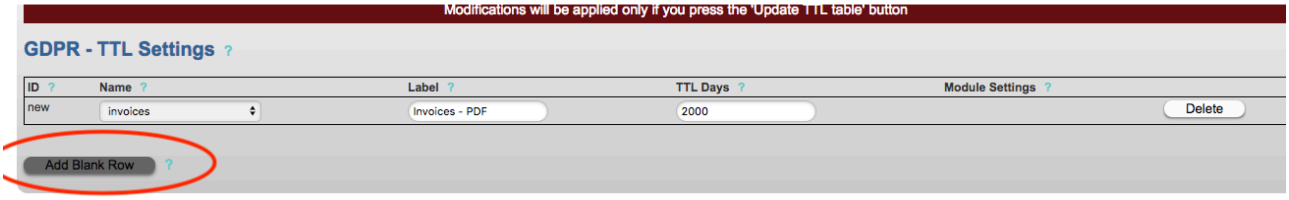


Fig. 3.2-3: GDPR: Time to Live Settings

By clicking on “Add Blank Row” as shown in Fig. 3.2-4 you can add a module.


Modifications will be applied only if you press the 'Update TTL table' button

GDPR - TTL Settings ?

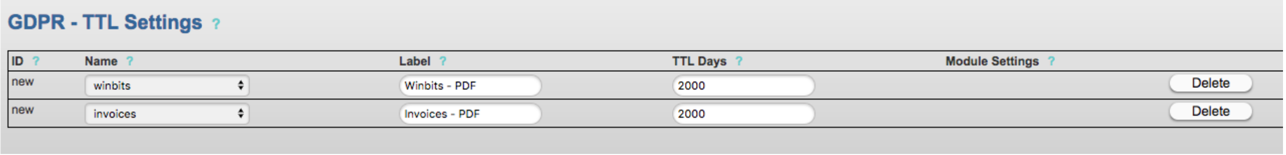
ID ?	Name ?	Label ?	TTL Days ?	Module Settings ?	
new	invoices	Invoices - PDF	2000		Delete

Fig. 3.2-4: GDPR: TTL Configuration

The modules currently available are listed below, and the number of modules available will increase over time.

1. **Invoices**: Allows operator to determine how many days old an invoice should be before being deleted. Please note that operators must review their legal requirements to hold on to financial information before deciding on the value to enter to this field.
2. **Winbits**: Allows operators to define after how many days a winbits file (direct debit file) should be deleted.

If for example, as in Fig. 3.2-5, the invoices and winbits files are set to be deleted after 2000 days, the operator must also schedule a script to run through and scan for invoices / winbits files that are ready for deletion.


GDPR - TTL Settings ?

ID ?	Name ?	Label ?	TTL Days ?	Module Settings ?	
new	winbits	Winbits - PDF	2000		Delete
new	invoices	Invoices - PDF	2000		Delete

Fig. 3.2-5: GDPR: TTL Settings

These automated scripts are configured on the Settings tab in SIMPLer in the section called "Cron Jobs" that is shown in Fig. 3.2-6.

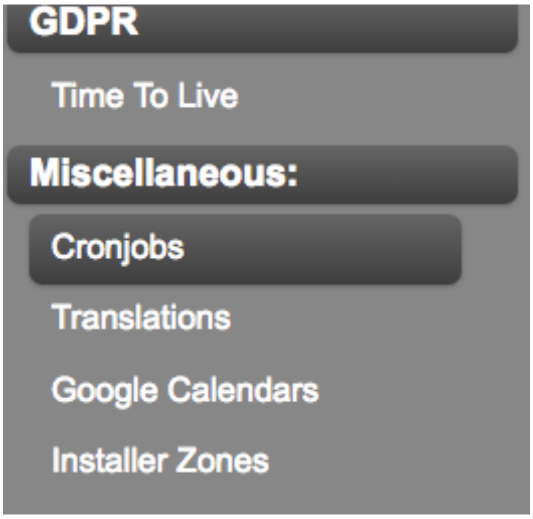
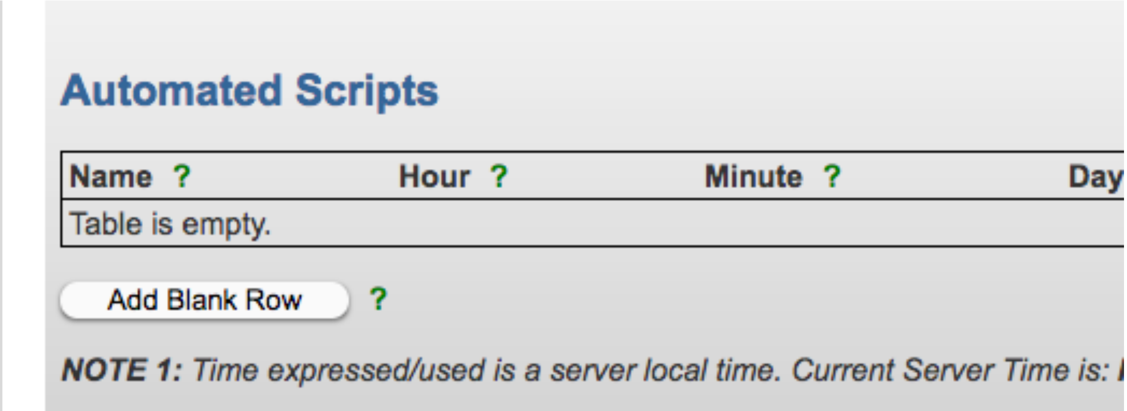


Fig. 3.2-5: Settings – Cron Jobs

Click "Add Blank Row" to add an entry to this table.



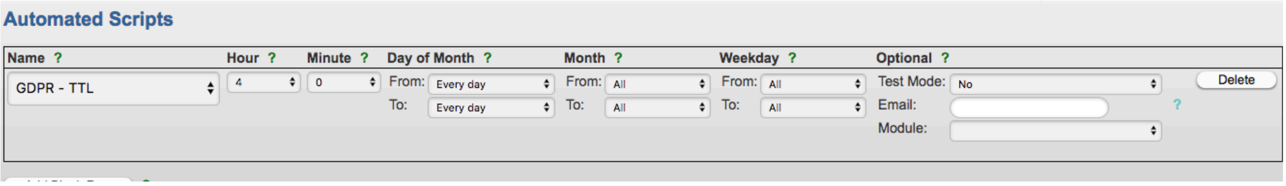
Automated Scripts

Name ?	Hour ?	Minute ?	Day
Table is empty.			

***NOTE 1:** Time expressed/used is a server local time. Current Server Time is:*

Fig. 3.2-6: Cron Jobs – Add Blank Row

1. Choose the script name "GDPR – TTL" from the drop-down menu.
2. Choose the hour and minute it should run at, for example for 4am please select "4" in the Hour section and "0" in the Minute section.
3. Choose the day of the month the script should run. For daily please leave "Every day" in the from and to section. For only on a specified day of the month such as the 12th please enter "12" to "12".
4. If you do not wish to run the script every month please choose specific months from the month drop-down.
5. If you do not wish to run the script every day of the week please choose specific weekdays from the weekday drop-down.
6. In the "optional" section please determine the module you wish to run, i.e invoices or winbits, specify which email address the results should be sent to and specify if the script should run in test mode or not.



Automated Scripts

Name ?	Hour ?	Minute ?	Day of Month ?	Month ?	Weekday ?	Optional ?	
GDPR - TTL	4	0	From: Every day To: Every day	From: All To: All	From: All To: All	Test Mode: No Email: Module:	Delete

Fig. 3.2-7: Cron Jobs – Configuration

When the script is run in test mode, an email will be sent to the address specified in Fig. 3.2-7 to show which files would be deleted.

If the live mode runs the files will be quarantined for 30 days before being fully deleted.

3.3 Right to be Forgotten

Operator can now easily deal with requests from operators for the Right to be Forgotten (RTBF)

A new section has been added to the customer record in SIMPLer on the left-hand side of the customer record. The new section is called “GDPR” and shown in Fig. 3.3-1. The relevant menu for the RTBF updates is called “Right to be Forgotten” and circled in Fig. 3.3-1.

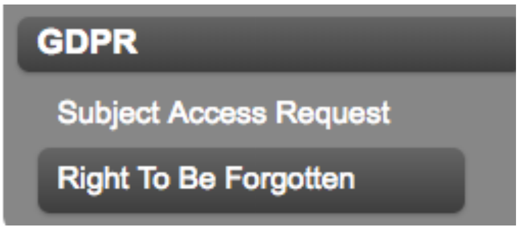
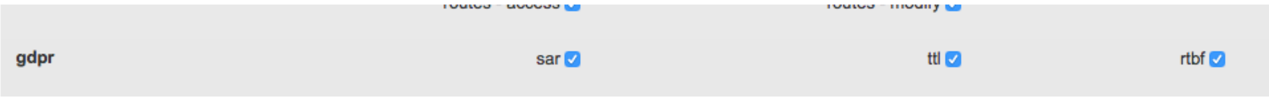


Fig. 3.3-1: GDPR: Right to be Forgotten

This section is driven by user rights on the user account. The section related to GDPR rights is called “gdpr” and the specific access right to use the Right to be Forgotten section is called “rtbf”.



gdpr	sar ☑	ttl ☑	rtbf ☑

Fig. 3.3-2: GDPR: Right to be Forgotten User Rights

By clicking on the “Right to be Forgotten” button shown in Fig. 3.3-1, the user can reach a console. This console presents several options to allow users to decide how customer information could be “forgotten”.

The two options are:

- Delete: This option shows rarely, it is available when the customer does not have any invoices attached to their record.
- Anonymize: Allows operators to **permanently** remove all personal information from the customer account.

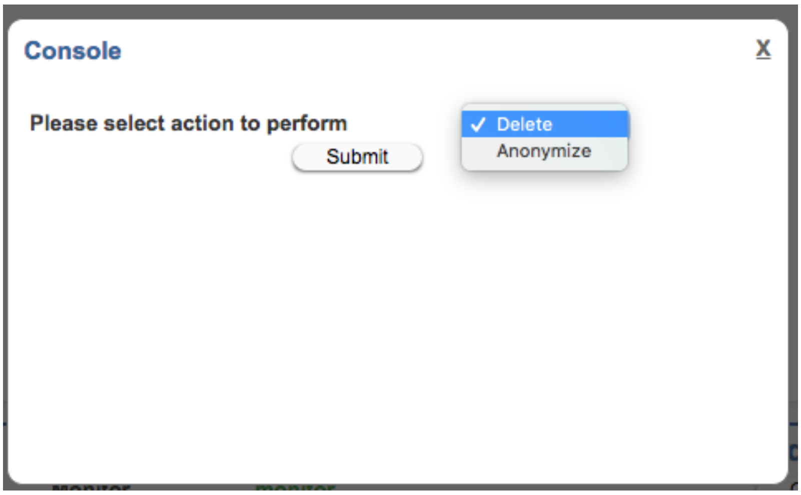
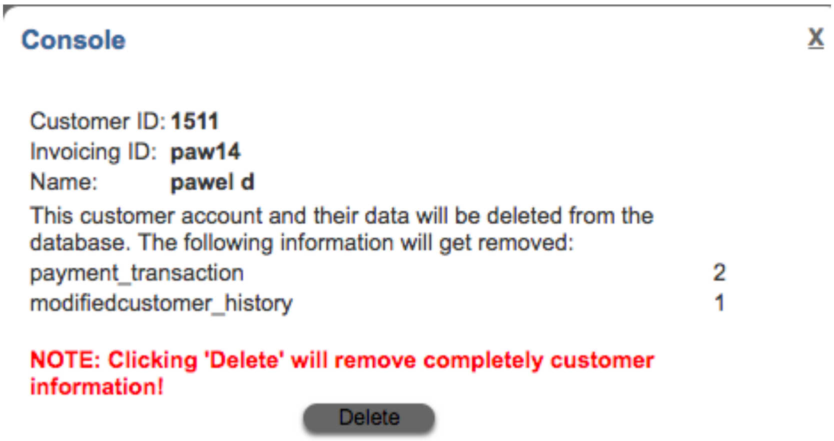


Fig. 3.3-3: GDPR: Right to be Forgotten Console

By selecting the “delete” option and clicking “submit” there is one final step to review the information to be deleted before clicking “delete” which will fully delete the account. This action will not be reversible.



Customer ID: **1511**
Invoicing ID: **paw14**
Name: **pawel d**

This customer account and their data will be deleted from the database. The following information will get removed:

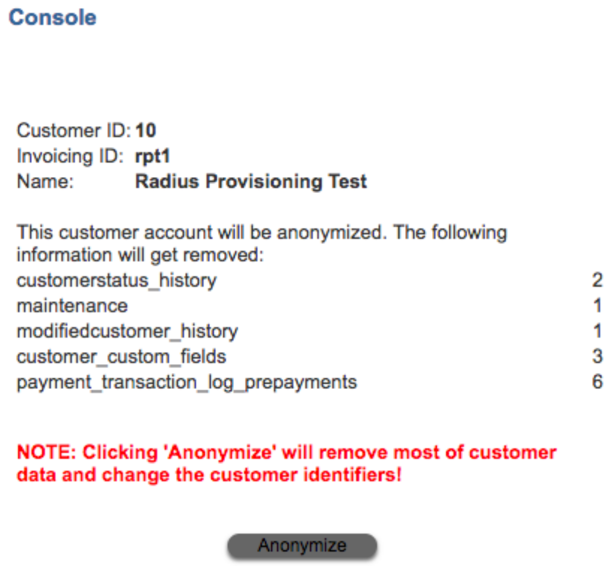
payment_transaction	2
modifiedcustomer_history	1

NOTE: Clicking 'Delete' will remove completely customer information!

Fig. 3.3-4: GDPR: Right to be Forgotten Delete Option

On accounts with invoice and payment data only “anonymize” will be an option. Or if “anonymize” is selected the process is as follows:

The console will summarise the details that will be changed. It will only show the changes made for this particular customer.



Customer ID: **10**
Invoicing ID: **rpt1**
Name: **Radius Provisioning Test**

This customer account will be anonymized. The following information will get removed:

customerstatus_history	2
maintenance	1
modifiedcustomer_history	1
customer_custom_fields	3
payment_transaction_log_prepayments	6

NOTE: Clicking 'Anonymize' will remove most of customer data and change the customer identifiers!

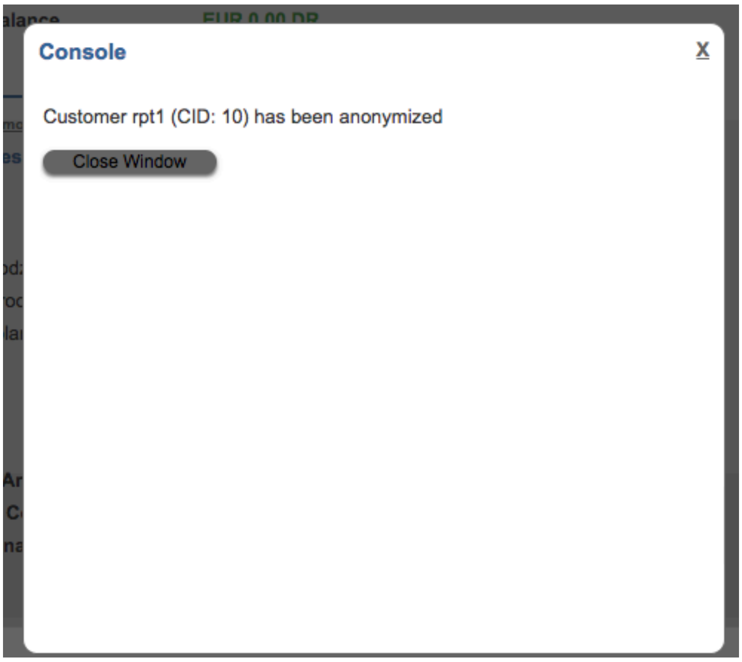
Fig. 3.3-5: GDPR: Right to be Forgotten Anonymize Option

The list of pages scrubbed/anonymized is below:

- Attachments
- Billing Issues
- Campaign Subscriptions
- CPE
- Credit Card
- Custom Fields
- Vouchers
- History
- EFT
- Electronic Documents
- Email Accounts
- EUP Logins
- Hotspot Users
- IP
- IP Archive
- Maintenance
- Modified customer history
- Notes
- Transaction Logs
- Payment Authorizations
- Sales Issues
- RADIUS Usernames
- Subscriptions (only if customers are deleted)
- Usage Log
- Usage Retention Log

After clicking "anonymize" the account will immediately become re-named in any areas where personal information is present. Some personal details will be removed and others will be renamed "RTBFXXX".

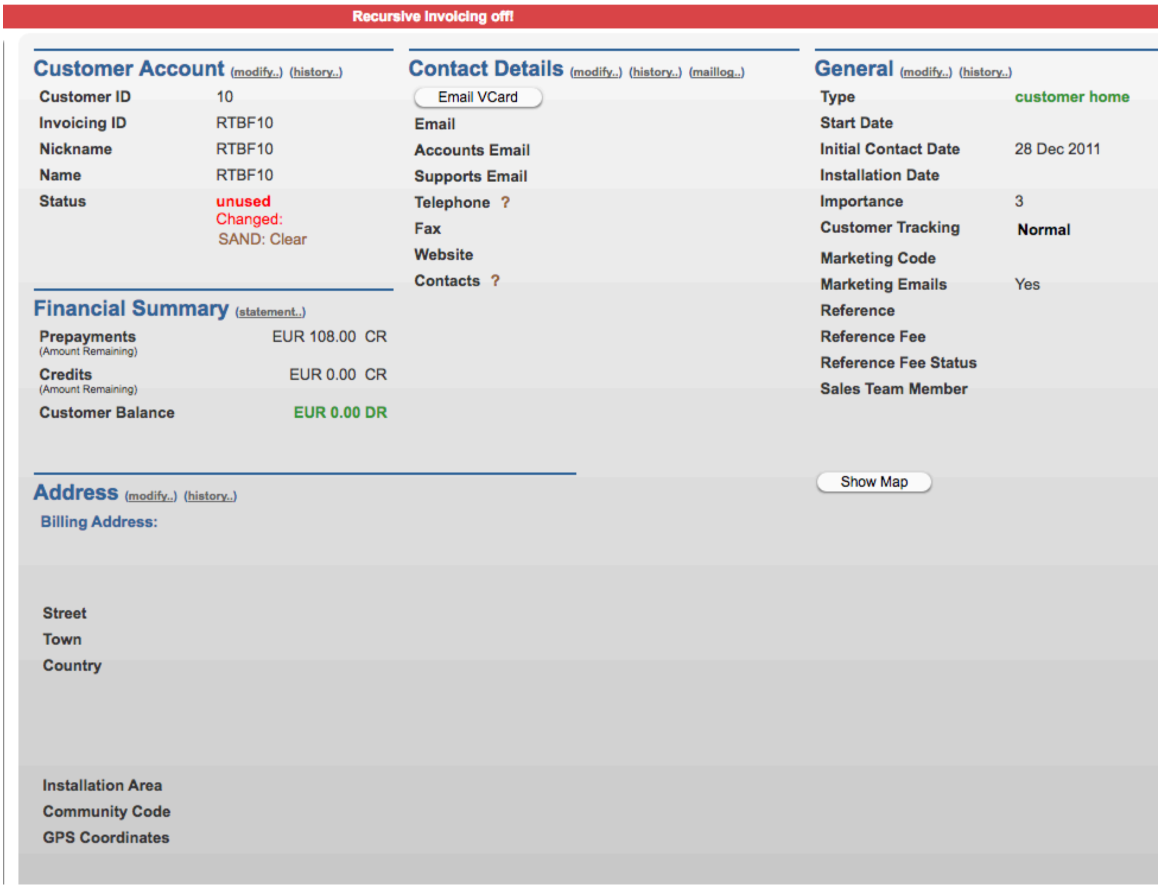
Invoices will no longer be accessible from this page.



Console

Customer rpt1 (CID: 10) has been anonymized

Fig. 3.3-6: GDPR: Right to be Forgotten Anonymize Confirmation



Recursive Invoicing off!

Customer Account (modify..) (history..)

Customer ID	10
Invoicing ID	RTBF10
Nickname	RTBF10
Name	RTBF10
Status	unused Changed: SAND: Clear

Financial Summary (statement..)

Prepayments (Amount Remaining)	EUR 108.00 CR
Credits (Amount Remaining)	EUR 0.00 CR
Customer Balance	EUR 0.00 DR

Contact Details (modify..) (history..) (maillog..)

Email VCard

Email	
Accounts Email	
Supports Email	
Telephone ?	
Fax	
Website	
Contacts ?	

General (modify..) (history..)

Type	customer home
Start Date	
Initial Contact Date	28 Dec 2011
Installation Date	
Importance	3
Customer Tracking	Normal
Marketing Code	
Marketing Emails	Yes
Reference	
Reference Fee	
Reference Fee Status	
Sales Team Member	

Show Map

Address (modify..) (history..)

Billing Address:

Street	
Town	
Country	
Installation Area	
Community Code	
GPS Coordinates	

Fig. 3.3-7: GDPR: Right to be Forgotten Anonymized Account

Annex A: References

A.1 Document References

A.2 Link References

[L1] http://www.azotel.com/

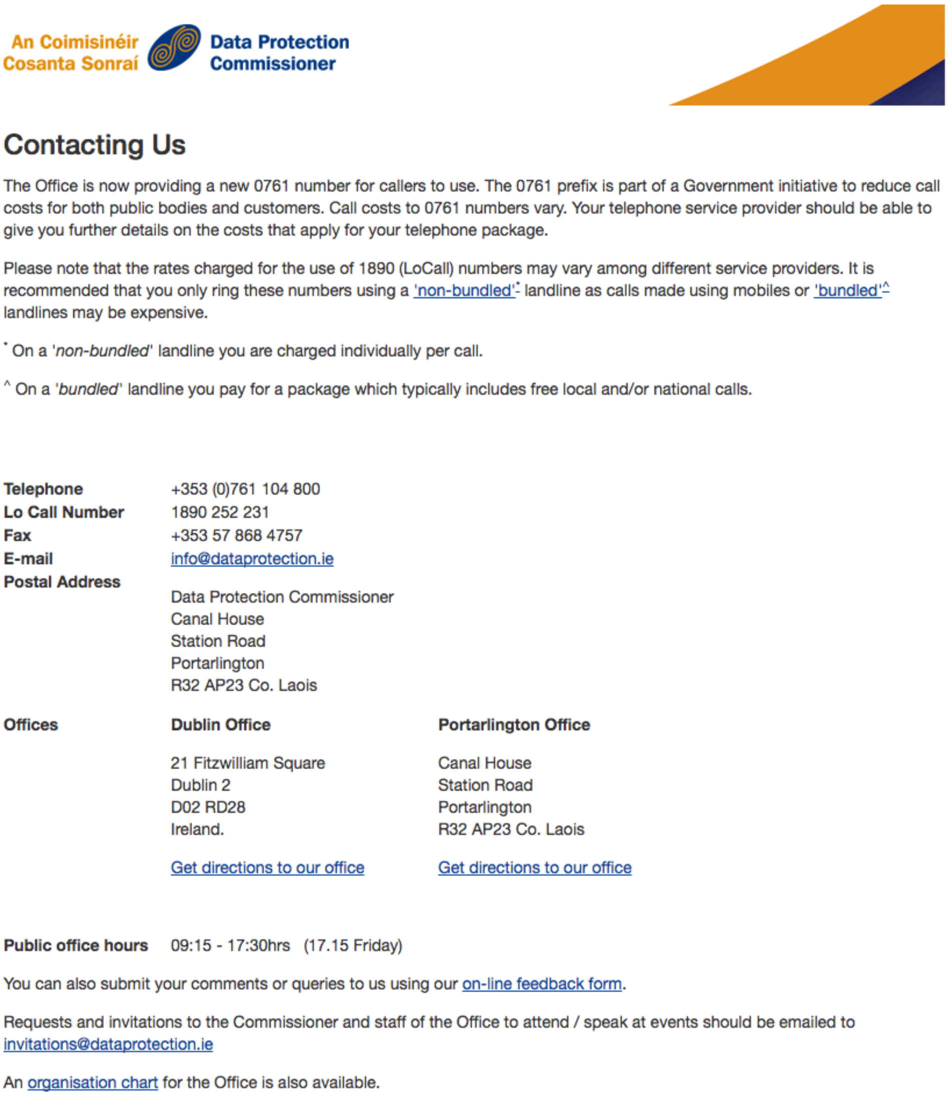
Azotel homepage.

[L2] http://www.eugdpr.org/eugdpr.org.html

Source of information in Section Two

[L3] https://www.dataprotection.ie/docs/EN/Contact-us/m/11.htm

Contact details for Irish Data Protection Commissioner.



Contacting Us

The Office is now providing a new 0761 number for callers to use. The 0761 prefix is part of a Government initiative to reduce call costs for both public bodies and customers. Call costs to 0761 numbers vary. Your telephone service provider should be able to give you further details on the costs that apply for your telephone package.

Please note that the rates charged for the use of 1890 (LoCall) numbers may vary among different service providers. It is recommended that you only ring these numbers using a 'non-bundled'* landline as calls made using mobiles or 'bundled'^ landlines may be expensive.

* On a '*non-bundled*' landline you are charged individually per call.

^ On a '*bundled*' landline you pay for a package which typically includes free local and/or national calls.

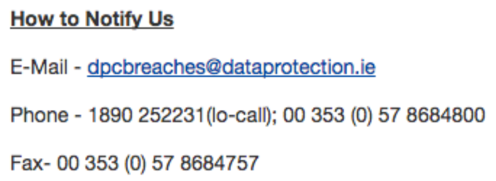
Telephone	+353 (0)761 104 800	
Lo Call Number	1890 252 231	
Fax	+353 57 868 4757	
E-mail	info@dataprotection.ie	
Postal Address	Data Protection Commissioner Canal House Station Road Portarlington R32 AP23 Co. Laois	
Offices	**Dublin Office**	**Portarlington Office**
	21 Fitzwilliam Square Dublin 2 D02 RD28 Ireland.	Canal House Station Road Portarlington R32 AP23 Co. Laois
	Get directions to our office	Get directions to our office

Public office hours 09:15 - 17:30hrs (17.15 Friday)

You can also submit your comments or queries to us using our on-line feedback form.

Requests and invitations to the Commissioner and staff of the Office to attend / speak at events should be emailed to invitations@dataprotection.ie

An organisation chart for the Office is also available.



How to Notify Us

E-Mail - dpcbreaches@dataprotection.ie

Phone - 1890 252231(lo-call); 00 353 (0) 57 8684800

Fax- 00 353 (0) 57 8684757

[L4] https://www.dataprotection.ie/docs/Home/4.htm

Irish DPCs website, for information.

Annex B: Definitions and abbreviations

B.1 Definitions

B.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

DPC	Data Protection Commissioner
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
SIMPLer	Azotel’s integrated Operators platform

Annex C: Change history

Change history				
Date	**Author**	**Subject/Comment**	**Old**	**New**
21 Nov 17	emma	Original	n/a	001
28 Nov 17	emma	Updated	001	002
20 Dec 2017	emma	Added RTBF	002	003