GDRP

MANUAL

OTYS Recruiting Technology

CONTENT

1 | INTRODUCTION

1.1 GENERAL

The General Data Protection Regulation (GDPR) replaces the Personal Data Protection Act (PDPA) with effect from 25 May 2018. In comparision to the PDPA, there are similarities but also a number of differences to be noted. These are mainly related to increasing the rights of those involved and increasing the responsibility of organizations to guarantee the privacy rights of the persons involved.

Both the PDPA and the GDPR are not new to OTYS. Our customers can easily work according to these laws, although sometimes via a detour or in our opinion too cumbersome. Precisely for this reason we have chosen to include the GDPR as a spearhead in our roadmap since Q3 2017.

This manual explains what requirements are covered by the GDPR, how OTYS deals with this and where the settings for the different automations can be found.

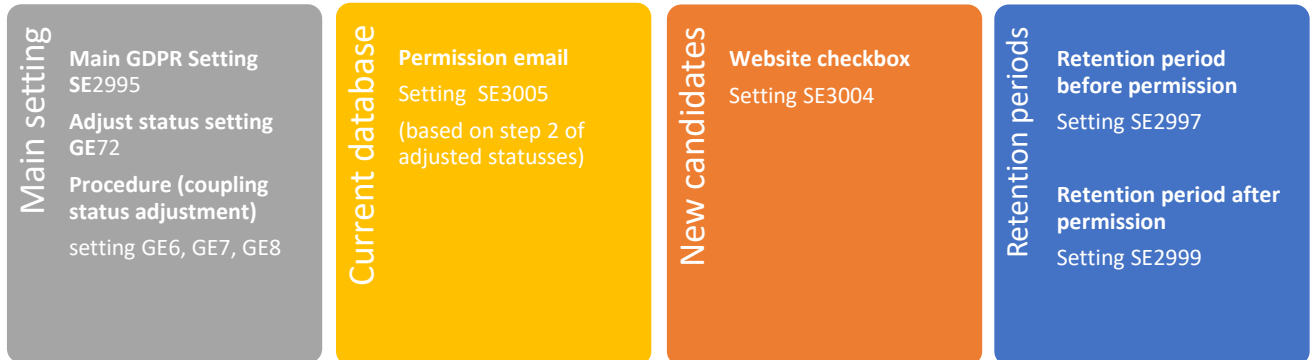## 1.2 ABOUT THE GDPR, SPECIFICALLY IN RECRUITING AND OTYS

Within the recruitment sector there are a number of elements to be aware of when it comes to legitimate data processing under the GDPR. The legal text (article 6) contains a number of conditions that must be met when it comes to the lawfulness of data processing:

- Permission
    - The consent request must be made clear and transparent
    - Must be given voluntarily (eg No mandatory permission request on application form, or completed check box)
    - Must be based on information, so it must be explained what is agreed with
    - Must consist of a statement of intent by which the person concerned accepts that personal data relating to him will be processed.
- Execution of an agreement
- Execution of a government task
- Vital interests of those involved
- Legal duty, for example employees and the obligation to provide data to the tax authorities
- Justified interest. You as a controller have a personal interest in the processing of personal data. Governments can not rely on this interest.

Thus, different conditions can be defined on the basis of which a legitimate data processing may take place. On this basis, the retention period is determined by the controller. To keep track of this period in an automated way, OTYS has developed a number of functionalities that can be activated through various institutions in OTYS Go!
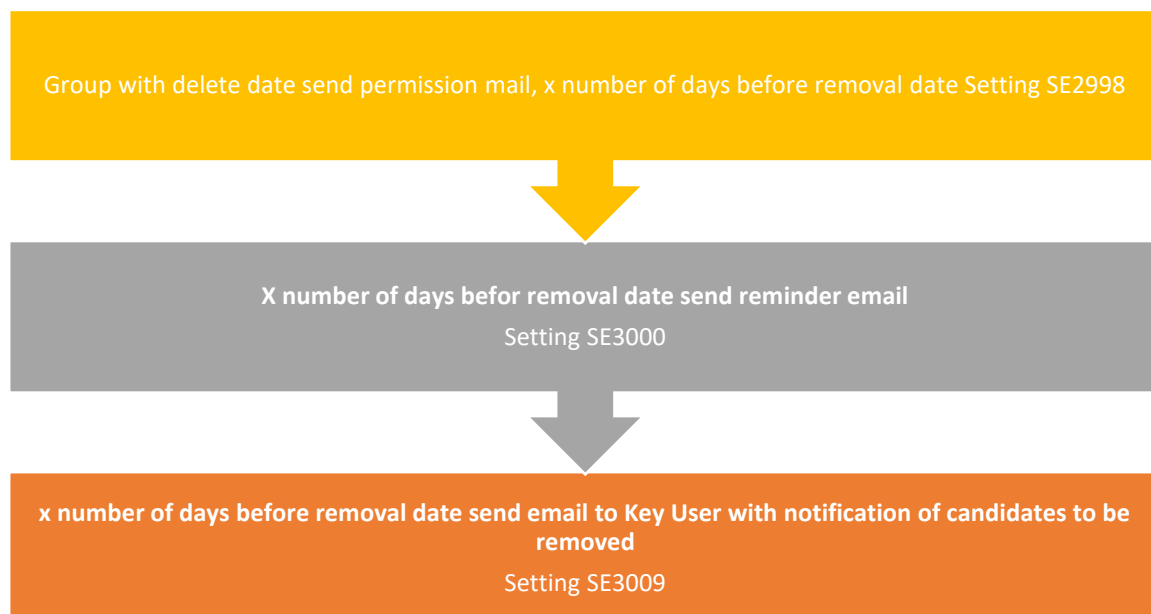
1.3 ABOUT THE AUTOMATED SOLUTION IN OTYS

In order for the automated GDPR solution to work for you, there are a number of settings that need to be activated or configured. Below you find an overview of these settings.

Main setting	Current database	New candidates	Retention periods
Main GDPR Setting SE2995 **Adjust status setting GE72** **Procedure (coupling status adjustment)** setting GE6, GE7, GE8	**Permission email** Setting SE3005 (based on step 2 of adjusted statusses)	**Website checkbox** Setting SE3004	**Retention period before permission** Setting SE2997 **Retention period after permission** Setting SE2999

By activating the settings above, removal dates will be linked to specific candidates. The manual for configuring the settings follows in the following chapters.

Based on the removal date, various e-mails will be sent, of which the sending date, intervals and content can also be set yourself:

Group with delete date send permission mail, x number of days before removal date Setting SE2998

⬇

X number of days befor removal date send reminder email
Setting SE3000

⬇

x number of days before removal date send email to Key User with notification of candidates to be removed
Setting SE3009

There are also various templates connected to the settings. These can always be found in the UTS Manager. The different names and numbers of the templates can be found in the following chapters.

1.4 LIST OF SETTINGS AND TEMPLATES

Client settings – from chapter 3 on, a comprehensive guide of how to configure these

⊖ GDPR

GDPR - Ask permission question for candidate question sets	Enabled		SE3004
GDPR - Enable automated permission emails	Enabled		SE3005
GDPR - Enable for client	Enabled		SE2995
GDPR - Interval in days for sending reminder email	3		SE3000
GDPR - Number of days before sending approval email	28		SE2998
GDPR - Period for saving candidate data after approval	12		SE2999
GDPR - Period for saving candidate data before approval	28		SE2997
GDPR - Require confirmation for killer question application forms	Disabled		SE3010
GDPR - Send Key-user notification email x days before deletion candidate	3		SE3009

Additional information in context of the GDPR

1.5   HOW DO I CONTROL MY RENTENTION PERIODS?

The retention period in OTYS starts when a removal date is assigned to a candidate. This date is granted in different ways, a number of which are discussed below:

The candidate applies via the website to a specific vacancy
- No permission: removal date on the day of the last email (term can be changed: setting SE2997 'retention period for permission')
- Permission is granted: removal date is set by default at 12 months after giving permission (term to be changed: setting SE2999 'retention period after permission')

The candidate registers via the website for an open application
Removal date is set by default at 12 months after applying for a job (term can be changed: setting SE2999 'retention period after permission')

Candidate is added manually, and a permission email is sent via button in candidate detail
- No permission: removal date on the day of the last mail (term to be changed: setting SE2997 'retention period for permission')
- Permission is granted: removal date is set by default to 12 months after giving permission (term to be changed: setting SE2999 'retention period after permission')

The removal date will be visible in the candidate list in the candidate module (after the general GDPR setting SE2995 has been activated, see chapter 4). Likewise, whether permission has been given. It is possible to filter on this removal date, so it is always clear which candidates will be removed soon.

The retention period of the current database is determined on the basis of different statuses and coupling statuses. More about this in chapters 3 and 4.

1.6   SECURITY OF OUR SOFTWARE

The GDPR states that both the controller and the processor 'take appropriate technical and organizational measures to ensure a level of security'. This level of protection must be attuned to the risks present.

The GDPR states that both the controller and the processor 'take appropriate technical and organizational measures to ensure a level of security'. This level of protection must be attuned to the risks present.

Taking appropriate measures is a broad concept. The following are the measures that OTYS will take in any case:

- Encryption of traffic from and to the database
- Up-to-date internal data protection policy
- Access security of premises, computers, network segmentation, firewalls, back-ups (also in other locations) and recovery policy to prevent 'loss' of data
- Automatic anonymization of personal data of candidates
- Codes of conduct, security awareness sessions for staff
- Comprehensive access control policies
- Annual SOC II audit by external auditor

> **NICE TO KNOW:**
> "Because the GDPR tells us to" does not apply to OTYS, we have been working on good data protection for years. We do want to make life easier for our customers because they have to do 'things' according to the GDPR. As a processor, we consistently have our software security in order.

1.7 TRANSFER OF DATA ABROAD

OTYS stores her and customer data within the EU (Belgium). For doing this, we use our subprocessor Sentia (UNITT). We have a subprocessor agreement with this subprocessor. The same applies to subprocessors Textkernel and Actonomy.

Textkernel: Processes data based on the resume parser. The personal data that is 'passed through' is processed by Textkernel, but not stored. We have made agreements about i.e. not providing any information to third parties.

Actonomy: we use Actonomy for our search functionality. To be able to use this search functionality properly, Actonomy uses the data in the database(s). We also have an agreement with this subprocessor in which agreements have been made about retention period, security and provision to third parties (not).

1.8 DATA BREACH

A data breach must be reported within 72 hours, after notification of the processor, to the regulator in your country. This means that OTYS must have a well-functioning process for communicating a data breach. This includes a number of points:

What is a data breach? - 'any breach of the security of personal data leading to any unauthorized processing thereof'

Report plan data leaks:
1. Within OTYS, this consists of a protocol that is tested annually to clarify who, where and when data leaks must be reported.
2. Report form data leaks to customers

3. Keep track of data leaks
4. In case of suspicion of a data breach, you can contact Bastiaan Brans via +31 (0) 318 584 900

1.9 RESPONSIBILITY

OTYS facilitates a lot of possibilities for its customers to deal with the GDPR in a good and fun way. However, we are not the party to impose retention periods and to impose the GDPR as legislation. Retention periods must be set by our customers themselves (otherwise standard guidelines are used). On the basis of these retention periods OTYS will perform its duty as processor. If other storage periods are used or GDPR settings are not used, OTYS cannot take responsibility for this.

By adding various widgets, reporting options and automated solutions, we hope that we can make the GDPR somewhat manageable. This manual however does not tell you everything that you as an organization have to do to comply with the GDPR. For more information on compliancy we refer you to the website of Data Protection Authority in your country.

2 | GENERAL GDPR SETTINGS

2.1 INTRODUCTION

According to the GDPR, it is mandatory to be able to submit permission from candidates who are already in a database. We offer you the possibility to request permission for the current database with the touch of a button. We think it is important that you can choose yourself who should or should not be asked. In this way you can use the various conditions that apply to lawful data processing under the GDPR (see chapter 1).

2.2 FUNCTIONALITY

OTYS has developed various settings that allow your database to operate automatically in line with the GDPR. The General GDPR setting is the start when taking the functionality into use. Setting SE2995 activates the GDPR functionality in the OTYS system. Once this functionality has been activated, the Key-user has 2 days to mark candidate statuses (setting GE72) to be involved in the GDPR process. In addition, the Key User must indicate the matching statuses indicating that a candidate has been rejected or accepted (settings GE6, GE7 & GE8).

Based on the configuration made, OTYS Go! automatically send e-mails to candidates to ask them if their data can be stored longer in the database. If the candidate does not take any action and the users of the system also take no action; the candidate will automatically be removed on the 'removal date' of the candidate. Please note that in order to allow Key-users time to properly organize the rest of the functionality, the functionality will only become active 2 days AFTER this setting has been activated.

2.3 STEPS TO BE TAKEN

Now that you know what the possibilities are for configuring the basic GDPR process, it is time to actually adjust the configuration in your OTYS system. To do this, take the following steps as Key-user.

1. Open OTYS Go!
2. Click on your name at the top right and choose 'Customer settings'
3. Search the top right of keyword 'gdpr'
4. Open setting 'GDPR - Activate for client' (setting SE2995)
5. Click on 'Active' and then click on 'Save'. The functionality will become active after 2 days, in the meantime there is the possibility to perform the following actions.
6. In the top right corner, search for keyword 'status'
7. Open 'Candidates - Candidate statuses' option (GE72 institution)
8. Open each status and take the following steps:

a. Place a checkmark in 'Keep' if you want the details of the candidate to be retained and no e-mails sent to the candidate. You can do this if you have a basis for retaining the data of candidates with this status without explicit permission from the candidate (for example with the status 'Working').

b. Place a checkmark at 'Delete' if you want the data of the candidate to be removed without permission emails sent to the candidate. You can do this if you prefer not to have the candidates with this status or in your database (for example with the status 'Not interesting').

c. If you do not use procedure statuses (see below), place a checkmark next to 'Posted' if this main status indicates that the candidate has been placed. We assume that all ongoing procedures are completed. As long as there are current placements, we will not ask the candidate for permission to keep his data. If there are no current placements, we will do this.

d. If you do not use procedure statuses (see below), place a checkmark at 'Rejected' if this main status indicates that the candidate has been rejected. We assume that all ongoing procedures are completed. As long as there are current placements, we will not ask the candidate for permission to keep his data. If there are no current placements, we will do this.

e. After your changes, click on the 'Save' button

9. Open setting 'Procedures - Procedure status 1' (setting GE6)
10. Open each status and take the following steps:
    a. Place a check mark at 'Rejected' if the procedure status indicates that the candidate has been rejected.
    b. After your changes, click on the 'Save' button
11. Repeat the above steps for the settings 'Procedures - Procedure status 2' & 'Procedures - Procedure status 3'.

You have now completed the basic settings of the GDPR process.

2.4 CHECKLIST

Check if you have taken all the steps by following the checklist:

- o Setting 'GDRP - Activate for client' setting activated
- o Candidate statuses of candidates who do not have to be removed automatically marked with 'Keep'
- o Candidate statuses of candidates who must be removed immediately marked with 'Delete'
- o No procedure statuses, candidate statuses indicating that a candidate is marked with 'Placed'
- o When no use procedure statuses, candidate statuses indicating that a candidate is rejected are marked with 'Rejected'
- o Procedure statuses indicating that a candidate has been rejected are marked with 'Rejected'
- o Procedure statuses indicating that a candidate has been hired are marked with 'Accepted'.

3 | CRM – DELETE CUSTOMERS

3.1 INTRODUCTION

We currently do not support a fully automated solution for customers. We are convinced that our (more) manual functionalities are sufficient to meet the GDPR in an efficient manner.

There are already several ways to approach, filter and delete customers. For example, based on last contact and based on registration date. You can also filter on CRM criteria. Registering permission can only be done manually by adding a CRM criteria. According to OTYS, this is sufficient at the moment because the CRM is often filled with customers (based on contract, work history and / or other) for which you can rely on the various conditions for processing personal data under the GDPR; see chapter 1.2.

We do offer the possibility to automatically delete customers. This will be done in the same way as the process for the candidate statuses and procedure statuses (see chapter 3). Only use GE74 (CRM - Customer status) for this. This will also happen 2 days after the general GDPR setting has been activated (see section 3.3).

3.2 FUNCTIONALITY

When linking customers statuses to 'delete', an automated process will also start 2 days after setting up the general GDPR functionality. All customer statuses that are linked to 'delete' will be removed. This happens in process during the night.

In this process not only the customers, but also the underlying contact persons including data will be removed.

3.3 STEPS TO BE TAKEN

After having set GDPR setting SE2995 (see chapter 3), you can follow the steps below. The functionality will become active after 2 days, in the meantime there is the possibility to perform the following actions.

1. Open OTYS Go!
2. Click on your name at the top right and choose 'Customer settings'
3. Search the keyword 'status' in the top right corner
4. Open 'CRM - Customer Statuses' setting (GE74 setting)
5. Open each status and take the next step:
    a. Place a check mark next to 'Delete' if you want the data of the customer (including the underlying contact data) to be deleted. You can do this if you prefer not to have

customers with this status in your database (for example with the status 'Not interesting').

     b. Click on the 'Save' button after making the changes

You have now configured the GDPR process for customers.

3.4 CHECKLIST

Check that you have taken all the steps using the following checklist:

o Customer statuses of customers that must be deleted immediately marked with 'Delete'.

4 | PROCESS EXCISTING CANDIDATES IN DATABASE

4.1 INTRODUCTION

Within the framework of the GDPR you have to ask candidates for permission if you want to keep their data in your database for purposes other than those for which the candidate provides them. For example, if a candidate applies for a vacancy, you can keep the details of the candidate as long as the procedure is running. Once the procedure has been completed, we will set a 'removal date' for the candidate. If you want to keep the details of the candidate for longer, you will have to ask permission for this.

If the steps in this chapter have been followed, the group of candidates you have selected will receive an e-mail in which the candidate is directed to a page on which he can give permission. If he does this he will be referred to his own profile page, where he can update his information. At the same time, a date will be attached in the database to the candidate on which the candidate will be removed.

If candidates have a removal date and are approaching it, you can choose to have the relevant Key user receive an e-mail containing an overview of the candidates to be automatically removed by OTYS. When the Key-user will receive this e-mail, you can also set the number of days in OTYS before the removal date.

Below is a complete explanation of the functionalities and associated settings.

4.2 FUNCTIONALITY

To ensure that existing candidates in your database automatically come into the right GDPR process, we have created the following settings that you can activate or modify:

GDPR - Activate automatic permission emails (setting SE3005)
The first e-mail is sent on a set number of days before the 'removal date' of the candidate (institution SE2998). If the candidate does not respond to this e-mail, reminder mail (s) can be sent with an adjustable interval (setting SE3000). So if this setting is activated, CSM setting SE2997 ('GDPR - Retention period for permission') is set to '28', CSM setting SE2998 ('GDPR - Number of days for sending permission mail') is set to '28' and CSM setting SE3000 ('GDPR - Interval in days for sending reminder emails') is set to '3'; After being rejected, a candidate will receive a 'removal date' of 28 days from now, he will receive an e-mail the same day with the request to keep his details and he will receive a reminder mail every three days (until he has agreed). with the retention of the data OR the candidate is automatically deleted on the removal date).

GDPR - Number of days for sending permission mail (institution SE2998)

By activating CSM institution SE3005, there is an automatic process that will send e-mails to candidates who are no longer in a procedure; to ask them for permission to keep their data. The first e-mail is sent on a pre-set number of days before the 'removal date' of the candidate, which can be adjusted via this setting. So if setting SE3005 is activated and this setting is '28', we will send an automatic permission email to the candidate 28 days before the removal date of the candidate.

GDPR - Interval in days for sending reminder emails (setting SE3000)

By activating CSM institution SE3005, there is an automatic process that will send e-mails to candidates who are no longer in a procedure; to ask them for permission to keep their data. The first e-mail is sent on a set number of days before the 'removal date' of the candidate (institution SE2998). If the candidate does not respond to this e-mail, reminder mail (s) can be sent with an adjustable interval that can be adjusted in this setting. So if setting SE3005 is activated, setting SE2998 is set to "28" and this setting is set to "3"; we will send an automatic consent email to the candidate 28 days before the candidate removal date and he will receive a reminder mail every three days (until he has agreed to retain the data OR the candidate is automatically deleted on the removal date).

GDPR - Send Key-user notification e-mail x days for deleting candidate (setting SE3009)

By activating customer institution SE3005, there is an automatic process that will send e-mails to candidates who are no longer in a procedure; to ask them for permission to keep their data. We prefer that candidates give their consent by sending them automatic e-mails and reminder e-mails. However, if a candidate does not respond to one of these e-mails, we want to inform Key-users before a candidate is removed. This setting (SE3009) determines the number of days before this Key-User notification e-mail is sent. So if this is set to '3' for example, we will send a notification e-mail to the Key-users for candidates who will be removed in three days. In this way, the Key-user (if applicable) can coordinate actions to prevent candidates being removed.

In addition, we have created the following templates:

GDPR - E-mail to candidate first request permission (template 1313)

This is the e-mail that is sent to a candidate to ask him for permission for the first time to keep his data in the database.

GDPR - E-mail to candidate first request permission (reminder) (template 1314)

This is the e-mail that is sent if a candidate has not responded to the above e-mail.

GDPR - E-mail to candidate repeat request permission (template 1316)

This is the e-mail that is sent if a candidate has not responded to the above e-mail.

GDPR - E-mail to candidate repeat request permission (reminder) (template 1316)

This is the e-mail that is sent if a candidate has not responded to the above e-mail.

GDPR - Form permission (template 1317)
This is the form that a candidate sees after clicking on a link in an e-mail, with which he can give permission to store his data in the database.

GDPR - Thank you page (template 1318)
This is the thank you page that someone sees after he or she has not given permission via the form above.

GDPR - Error message (template 1319)
This is the error page that someone sees if something goes wrong in the above process.

GDPR - E-mail to Key-user x days for deleting candidate (template 1323)
This is the e-mail that is sent to the Key-user to inform him about candidates that will be removed soon.

> **GOOD TO KNOW:**
> As an OTYS user you can manually extend the removal date of a candidate. You will then have to indicate that the candidate has given explicit permission for this.

4.3 STEPS TO BE TAKEN

Now that you know what the possibilities are for configuring the GDPR process for existing candidates, it is time to actually adjust the configuration in your OTYS system. You take the following steps as Key-user.

First you change some settings in your customer settings:
1. Open OTYS Go!
2. Click on your name at the top right and choose 'Customer settings'
3. Search the top right of keyword 'gdpr'
4. Open 'GDPR - Activate automatic consent mail' settings (setting SE3005)
5. Click on 'Active' and then click on 'Save.
6. Open setting 'GDPR - Number of days for sending permission mail' (setting SE2998)
7. This option is set to '28' by default. If necessary, change this to a different number and then click on 'Save'.
8. Open 'GDPR - Interval in days for sending reminder emails' (setting SE3000)
9. This option is set to '28' by default. Change this if desired to a different number and then click on 'Save'.
10. Open setting 'GDRP - Send Key-user notification e-mail x days for deleting candidate' (setting SE3009).

11. This option is set to '3' by default. Change this if desired to a different number and then click on 'Save'.

If you do not want to apply the GDPR process for your existing candidates at all, you will have to ensure that (1) all candidates in your database have a main status and (2) in all these statuses the option 'Save' is checked.

After you have adjusted the above settings, you can still change the standard texts used on your website:

1. Open OTYS Go!
2. Click on the OTYS logo and click on the UTS Manager
3. Search by keyword 'gdpr'
4. Open the template that you want to modify
5. On the top right, set the language to the desired language
6. Click on the change icon next to the text that needs to be changed
7. Change the text as desired on the right-hand side of the screen in the 'Translation' block.
8. Click on the Save icon in the upper right corner of the 'Translation' block
9. Repeat these steps for other texts that you want to adjust

A review of the templates to be adjusted can be found in section 4.2.

4.4 CHECKLIST

Check that you have taken all the steps through the following checklist:

- o 'GDPR - Activate automatic consent emails' setting activated
- o Setting 'GDPR - Number of days for sending permission mail' adjusted, if desired
- o Adjust 'GDPR - Interval in days for sending reminder emails', if desired
- o Setting 'GDPR - Send Key-user notification e-mail x days for removal of candidate' adjusted, if desired
- o Template 'GDPR - Form permission' adapted, if desired.
- o Template 'GDPR - Thank you page' adapted, if desired.
- o Template 'GDPR - Error message' adjusted, if desired.
- o Template 'GDPR - E-mail to candidate first request permission' adjusted, if desired.
- o Template 'GDPR - E-mail to candidate first request permission (reminder)' adjusted, if desired.
- o Template 'GDPR - E-mail to candidate repeat request permission' adapted, if desired.
- o Template 'GDPR - E-mail to candidate repeat request permission (reminder)' adjusted, if desired.
- o Template 'GDPR - E-mail to Key-user x days for removal of candidate' adjusted, if desired.

5 | PROCESSING PROCESS FOR NEW CANDIDATES

5.1 INTRODUCTION

In this chapter we will explain how you can configure the GDPR process for new candidates in OTYS (ie candidates who are not yet in your database, but will soon be in your database because they are applying for a vacancy on your website, for example). We will first explain what functionality we have created for this and then show you step-by-step how you activate this functionality and adapt it to your preferences. We conclude with a checklist so that you can be sure that you have taken all the steps.

5.2 FUNCTIONALITY

In order to ensure that new candidates in your database automatically come into the right GDPR process, we have created the following settings that you can activate or modify:

GDPR – Request permission in candidate question sets (institution SE3004)
By activating this setting, a question will be added at the bottom of the candidate question set, to ask the candidate whether his data may be stored for a certain time in the database (due to GDPR / AVG legislation) if the candidate applies for a vacancy. The content of this checkbox & text within this question can be changed in UTS template 1311. If the candidate ticks (and thus agrees) the checkbox, the candidate's data is stored for the number of months as configured in CSM client setting SE2999 (standard 12 months).

GDPR - Retention period after permission (institution SE2999)
Within the framework of the GDPR / AVG you have to ask candidates for permission if you want to keep their data in your database for purposes other than those for which the candidate provides them. For example, if a candidate applies for a vacancy, you can keep the details of the candidate as long as the procedure is running. If the procedure has been completed and you still want to keep the details of the candidate, you will have to ask permission for this. After the candidate has given permission, the data is saved for a certain period. This period therefore applies to candidates who apply for a vacancy via the website, respond via an open application or give permission via the automated mail solution from OTYS (see chapter 5). Through this institution you determine what this period is in months (standard '12', based on Dutch GDPR / AVG guidelines).

GDPR – Retention period before permission (institution SE2997)
Within the framework of the GDPR / AVG you have to ask candidates for permission if you want to keep their data in your database for purposes other than those for which the candidate provides them. For example, if a candidate applies for a vacancy, you can keep the details of the candidate as long as the procedure is running. If the procedure has been completed and you still want to keep the details of the candidate, you will have to ask permission for this. Through this institution you determine the number of days that OTYS must store the data of the candidate (standard '28', based

on Dutch GDPR / AVG guidelines). So if it is set to '28', a candidate who has been turned down for a vacancy (and has no other procedures running) will be kept in the system for 28 days. If the candidate does not agree that his data will be kept longer (see institution SE2999); the details of this candidate will be deleted after this period.

In addition, we have created the following template:

GDPR - Keeping an agreement on data when applying (H) (template 1311)
This is the template of the text that the candidate sees when he applies for a vacancy and 'agrees' to keep his data longer in the database.

5.3   STEP TO BE TAKEN

Now that you know what the possibilities are for configuring the GDPR process for new candidates, it is time to actually adjust the configuration in your OTYS system. Take the following steps as a Key-user.

First you change some settings in your customer settings:

1. Open OTYS Go!
2. Click on your name at the top right and choose 'Customer settings'
3. Search the top right of keyword 'gdpr'
4. Open 'GDPR - Request for permission in candidate question sets' (institution SE3004)
5. Click on 'Active' and then click on 'Save. From now on, a checkbox and accompanying text will be displayed at the bottom of the application form on your website. This permission is visible in a candidate detail.
6. Open 'GDPR - Retention period after permission' setting (setting SE2999)
7. Enter the desired number of months and click on 'Save'. By default, this is set at 12 months (guideline AVG), but we receive signals from customers that they want to set it differently. Think carefully about this!
8. Open 'GDPR - Retention period for consent' setting (setting SE2997)
9. Enter the desired number of days and click on 'Save'. By default, this is 28 days (AVG directive), but we receive signals from customers that they want to set it differently. This is possible, but think about this carefully!

You can (if desired) adjust the contents of the above checkbox & text:
1. Open OTYS Go!
2. Click on the OTYS logo and click on the UTS Manager
3. Search by keyword '1311'
4. Open the template 'GDPR - Keeping an agreement on data when applying for a job (H)'
5. On the top right, set the language to the desired language
6. Click on the change icon next to the text that needs to be changed

7. Change the text as desired on the right-hand side of the screen in the 'Translation' block. The displayed tag {$ gdprLongTermMonths} shows the number of months that each OTYS customer can configure himself and on the basis of which the data will be retained.
8. Click on the Save icon in the upper right corner of the 'Translation' block
9. Repeat these steps for other texts that you want to adjust

Finally, check on your website if everything is logically arranged by doing one or more test applications yourself. This question is only asked if one applies for a vacancy. If a candidate makes an open application / enrollment, the longer retention period will automatically be used.

5.4 CHECKLIST

Check that you have taken all the steps through the following checklist:

- o 'GDPR - Request for permission in candidate question sets' option (setting SE3004) activated.
- o Determined whether you want to keep the standard retention period after permission (12 months) or depart from it.
- o 'GDPR - Retention period after permission' setting (SE2999 setting) adjusted (if applicable).
- o Determined whether you want to keep the standard retention period after permission (12 months) or depart from it.
- o 'GDPR - Retention period for consent' setting (setting SE2997) adjusted (if applicable).
- o Textual changes to UTS template 'qGdprAcceptViewH.html' (template 1311).
- o Some test applications made to check process.

6 | ADDITIONAL FUNCTIONALITIES

6.1 AUTOMATED REMOVAL PROCESS

The removal of candidates takes place once every 24 hours, at night. Deleting within OTYS means that the personal data will be deleted, but that the non-personal data can still be used for reporting. After removal, the candidates can no longer be found in the candidate module and this also can NOT be canceled.

6.2 VIEW REMOVAL DATE OF CANDIDATE

In OTYS Go! on the left side of a candidate detail you will see the 'removal date' of the candidate. If the candidate does not have a removal date (i.e. because he is still part of a process), this is showed on a label (in the later example the label will be: 'in procedure, not set'). If you click on this date (or label) a window with additional options will open.
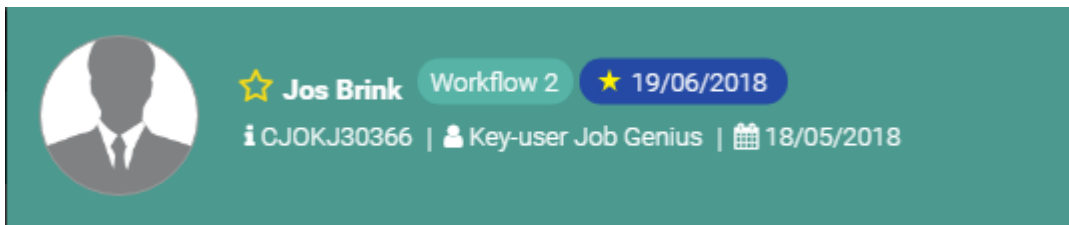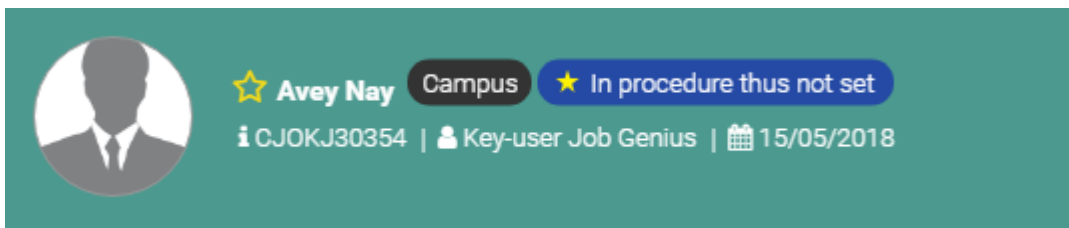
GDPR Tools   ⊗

| Due Date | 19 Jun 2018   📅 | Set Due Date |

Cancel   Send permission email   Send candidate data   Export GDPR activity log

6.3 MANUALLY CUSTOMIZING THE REMOVAL DATE FOR CANDIDATE

If you receive explicit permission from the candidate to keep his details in another way (for example by e-mail or via WhatsApp), you can manually change the removal date of a candidate. After you have clicked on the removal date or on the label in a candidate detail (see section 8.2), a window opens with additional options. Change the removal date here and then click on 'Set expiry date'. In addition, we advise you to store the 'proof' of the explicit permission (for example a screenshot of the agreement via WhatsApp) in the candidate's file.

| Due Date | 19 Jun 2018   📅 | Set Due Date |

6.4 MANUALLY ASK FOR PERMISSION (ALSO VIA LINKEDIN)

Some candidates will ask you for permission via another route because you entered them manually or because you put them in OTYS via LinkedIn. After you have clicked on the removal date or on the label in a candidate detail (see section 8.2), a window opens with additional options. Click on the 'Send' button under 'Consent e-mail' to send this permission e-mail. The e-mail opens to the candidate and you can adjust the e-mail before sending it. Via this way the candidate will be able to give permission as well, if he gives permission he will be referred to his own profile page, where he can update his information. At the same time, a date will be added in the database to the candidate on which the candidate will be removed.

To see this button, the general GDPR settings SE2995 must be activated. Note: if this setting is activated, the Key user has 2 days to configure the settings.

The standard text of the email that is sent can be modified in UTS template 'GDPR - E-mail to candidate after asking permission manually' (template 1324).
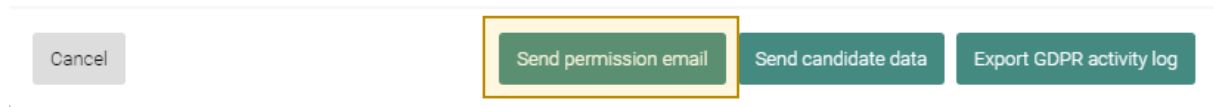

6.5 DOWNLOADING DOSSIERS

Under the GDPR, it must be possible to give a candidate access to the data that is stored. OTYS has the following solution for this.

With a press of a button it is possible to generate a zip file, which can be sent to the relevant candidate as an attachment in an email. This zip-file contains the data that the candidate has provided, and mail traffic between your organization and the candidate.

It is possible to delete certain file items; but this is not possible with some file items. For example, it is possible to delete notes and documents from a file, but it is not possible to delete emails.

After you have clicked on the removal date or on the label in a candidate detail (see section 8.2), a window opens with additional options. Click on the 'Send data' button under 'Candidate details' to send this e-mail. The e-mail opens to the candidate and you can adjust the e-mail before sending it. The text of this e-mail can be changed. To view this button, the general GDPR settings SE2995 must be activated. Note: if this setting is activated, the Key user has 2 days to configure the settings. The standard text of the e-mail that will be sent can be adjusted in UTS template 'GDPR - E-mail to candidate with data candidate' (template 1325).
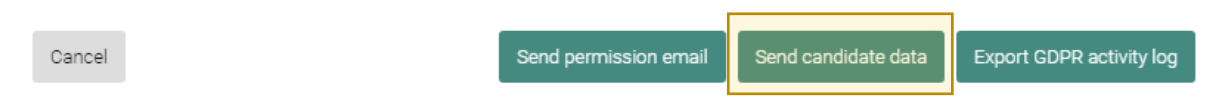

6.6 ACTIVITEITENLOGBOEK DOWNLOADEN

In addition to the options mentioned above, it is also possible to download a log from when the 'delete date' has been modified and by whom this change has been implemented. After you have clicked on the removal date or on the label in a candidate detail (see section 8.2), a window opens with additional options. Click on 'Export' in 'GDPR activities log' to download this e-mail. A CSV file is then downloaded with the details of all changes to the removal date of candidates.
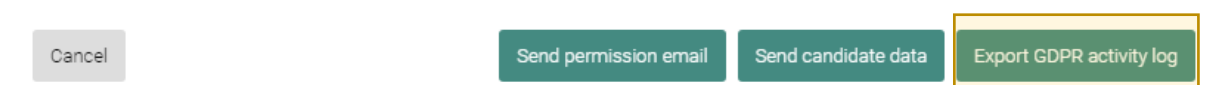
6.7 CONFIGURE FILTERS & WIDGETS

In the search filter of the Candidates module of OTYS Go! you will find an extra option to search for candidates with a certain 'removal date'. This allows you to make a search with, for example, all candidates that will be removed in the next seven days (possibly supplemented with a specific owner). In OTYS Go! you can save a search as 'filter' so you can easily access such a list and you can configure a widget on your dashboard to display this list directly on your dashboard. More information about these functionalities can be found in the manuals 'Lists, search & match' and 'Dashboard module'.

Followup	⊕
GDPR Due Date	⊕
Gender	⊕
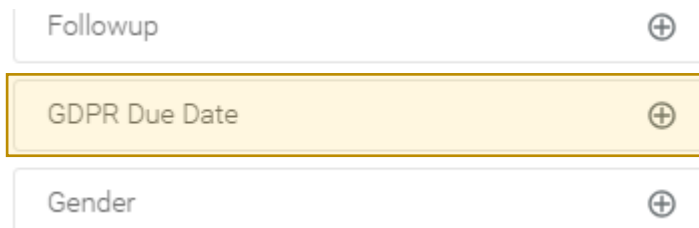
7 | PROCESS IN CASE OF NO OTYS WEBSITE

Even if you do not have an OTYS website, you can use our GDPR functionality. In that case, after clicking on a link in an email, candidates will be referred to a general website where they can indicate their preferences.

In this case, other UTS templates are used than the templates discussed in section 4.2. The following templates are used in this case:

GDPR - Form permission (fallback in case of no OTYS website) (template 1320)
This is the form that a candidate sees after clicking on a link in an email, with which he can give permission to store his data in the database.

GDPR - Thank you page (fallback at no OTYS website) (template 1321)
This is the thank you page that someone sees after he or she has not given permission via the form above.

In addition, it is possible for an external party to consult or change the removal date of a candidate via our web services. Your external party will find the field definitions in the list of definitions of our web services.

Should your external party have any questions when implementing the above, we would please like to hear that.