# Guide for iCIMS Talent Platform Customers to Certain GDPR Compliance Functions

On May 25, 2018, the EU's next generation of data protection law, the General Data Protection Regulation (the "GDPR"), went into effect. The GDPR aims to strengthen the security and protection of personal data and replaces the 1995 European Union Data Protection Directive.

The GDPR imposes requirements both on "controllers" (those who determine the purposes and means of processing personal data, such as iCIMS customers) and "processors" (those who process personal data on behalf of a controller, such as iCIMS).

The purpose of this document is to explain how the iCIMS Talent Platform supports iCIMS customers in complying with GDPR requirements regarding:

- Lawful processing and consent of data subjects
- Data subject rights, including:
  - Right to erasure of personal data
  - Data access rights
  - Rectification and correction of data
  - Restriction of processing
  - Portability of data

## Consent

### New Candidate Consent

The customer has the option to determine whether to capture consent from all new candidates, from only candidates who self-identify as EU residents, or from no new candidates. The customer must supply its approved consent language.

To support the customer in collecting consent from new candidates, customers may configure each portal in one of three ways:

1. Present a field requesting consent to all new candidates. In this configuration, all new candidates are presented with the opportunity to provide opt-in consent for the proposed usage of their data.
2. Present a field requesting consent only to new candidates who indicate that they are a resident of the EU. In this configuration, the new candidate is asked to identify whether they are an EU resident. For new candidates who identify as EU residents, the portal gives the candidate the opportunity to provide opt-in consent for the proposed usage of their data.
3. Not present a field requesting consent to any new candidate. In this configuration new candidates are not asked to consent.

For configurations where some or all new candidates are required to indicate their consent (i.e., options one and two in the list above):

- The consent is requested before any personal data is captured.
- Consent is only recorded if the candidate affirmatively opts-in to consent by checking a checkbox (which is not pre-filled).
- The timestamp for consent, as well as the consent verbiage, is captured for the candidate and retained in a data table.
- If the candidate does not provide consent, then the candidate is not permitted to proceed with the application process and no personal data is captured.
- Enablement of notification (see below) is independent of enablement of consent.

***Note:*** *These features do not replace or modify any other consent features available in the iCIMS Talent Platform, such as the capture of consent to conduct background screening.*

## Pre-Existing Candidate Consent

The customer has the option to determine whether to capture consent from existing candidates. These candidates can include candidates already in the iCIMS Talent Platform prior to the GDPR compliance date, or candidates who were imported from another system where the candidate existed prior to the GDPR compliance date. The customer has the same configuration options as for new candidates (See previous *New Candidate Consent* section) and can control the portal configuration option for existing candidates separately from new candidates.

For configurations where some or all existing candidates are required to indicate their consent to processing:

- If the customer chooses to request consent, then the portal presents a field requesting consent when the existing candidate next logs in to the portal after the configuration is turned on.
- The customer is responsible for prompting existing candidates (e.g., sending an email request) to return to the portal, log in, and provide consent. This is not an automated process, and the customer should ensure an appropriate process is in place for existing candidate return requests.
- If the returning candidate does not provide consent, this information is visible in the customer system within a personal data request report. This report has pre-configured default templates, which can be modified as needed. The customer may enable a scheduled report to be emailed to a person from the customer's organization for review and processing. The customer will need to determine whether deletion of candidate data should proceed.
- If the customer determines that deletion will proceed, then the customer must move the candidate into a purge status, which will delete the candidate's data during the next purge cycle. To initiate the purge cycle, the customer may make the request through customer support or trigger the purge cycle directly (if they have previously requested the ability to trigger a purge themselves).

### Additional Details on Purging

- Candidate data that a controller must retain can be exported prior to deletion. All candidate data will be deleted from the iCIMS Talent Platform upon a purge.
- Candidate profiles are scheduled for purge by putting the profile into the purge status and then confirming that a purge should run during an upcoming purge window. The ability to schedule a purge can be extended to the user admins of the system. Otherwise, a request can be submitted to iCIMS Technical Support to schedule the purge.
- If a candidate profile has been mistakenly or prematurely marked for purge, the user admin can remove the candidate profile from the purge status if this action is taken prior to the purge running.
- Note that purges take place during off hours and do not run immediately. (For more information, see https://care.icims.com/s/article/Purging-Person-Profiles.)
- The customer should ensure appropriate processes are in place to initiate purge requests.

## Removal of Consent

Candidates are able to remove consent by logging in to the portal and accessing a new page linked from their dashboard that allows the candidate to submit this type of request.

- When a candidate revokes consent, it locks their access to the portal, limiting them to only making GDPR-related requests.
- Requests from candidates are visible in the customer system within a personal data request report. This report has pre-configured default templates, which can be modified as needed. The customer may enable a scheduled report to be emailed to a person from the customer's organization for review and processing.
- Processes related to 'Right to Restriction of Processing' and 'Right to Erasure/Right to be Forgotten,' as identified below, should be

followed in order to ensure that data is no longer processed and is completely removed from the system.

- The customer should provide confirmation directly to the candidate.
- The customer should ensure appropriate processes are in place to address removal of consent requests.

# Notification

## New Candidate Notice

The customer has the option to determine whether to provide a notice from the customer to all new candidates, to only new candidates who self-identify as EU residents, or to no new candidates. This notice can be enabled separately from consent, if desired. The customer must supply its own notice language.

To support the customer in presenting the desired notice to new candidates, customers may configure each portal in one of three ways:

1. Present the customer's notice to all candidates. In this configuration, all new candidates are presented with a notice regarding how the customer will use the candidate's data.
2. Present the customer's notice only to new candidates who indicate that they are a resident of the EU. In this configuration, the new candidate is asked whether they are an EU resident. The portal presents the notice only to new candidates who identify as an EU resident.
3. Not present notice to any new candidate. In this configuration new candidates are not presented with a notice from the customer.

For configurations where some or all new candidates are presented with the customer's notice (i.e., options one and two in the list above):

- The candidate must be presented with the notice in order to proceed with the application process. No data is captured prior to the notice being presented.
- If the candidate chooses to proceed with the application process after the notice is reviewed, the time stamp and actual message in the notice are stored in the data table in addition to consent information, if consent is enabled.
- No response or opt-in are required for the notice. The notice, however, is presented on the page prior to the candidate being allowed to proceed to the next page.

***Note:*** *These do not replace or modify any other consent features available in the Platform, such as existing ability to provide notices through text, links, or otherwise.*

## Pre-Existing Candidate Notice

The customer has the option to determine whether to provide a notice from the customer to candidates already in the iCIMS Talent Platform prior to the GDPR compliance date, and to candidates who were imported from another system where the candidate existed prior to the GDPR compliance date. The customer has the same configuration options as for new candidates (See previous *New Candidate Notice* section) and can control the portal configuration option for existing candidates separately from new candidates.

For configurations where some or all existing candidates are presented with the customer's notice:

- If the customer chooses to provide notice, then the notice will be presented when the existing candidate next logs in to the portal after the configuration is turned on.
- The customer is responsible for prompting existing candidates (e.g., sending an email request) to return to the portal and log in to review the notice. This is not an automated process, and the customer should ensure an appropriate process is in place for existing candidate return requests.

# Candidate Data Subject Rights

The iCIMS Talent Platform allows customers to configure the methods used to address data subject (in this case, the "candidate") rights. These features may be set per-portal and can be displayed to all candidates, only self-identified EU residents, or no candidates.

## Right to Erasure/Right to be Forgotten

If enabled, candidates are able to submit a request to have their information deleted from the system by logging in to the portal. There is a page accessible via the candidate dashboard that allows the candidate to submit this type of request. The candidate may enter an optional message with additional details as part of the request submission.

Requests from candidates are visible in the customer system within a personal data request report. This report has pre-configured templates which can be modified as needed. The customer may set up a scheduled report to be emailed to a person from the customer's organization for review and processing.

- Candidate data that a controller must retain can be exported prior to deletion using existing functionality. All candidate data will be deleted from the iCIMS Talent Platform upon a purge.
- Candidate profiles are scheduled for purge by putting the profile into the purge status and then confirming that a purge should run during an upcoming purge window. The ability to schedule a purge can be extended to the user admins of the system. Otherwise, a request can be submitted to iCIMS Technical Support to schedule the purge.
- If a candidate profile has been mistakenly or prematurely marked for purge, the user admin can remove the candidate profile from the purge status if this action is taken prior to the purge running.
- Note that purges take place during off hours and do not run immediately. (For more information, see https://care.icims.com/s/article/Purging-Person-Profiles.)
- The customer should ensure appropriate processes are in place to initiate purge requests.

## Right to Access

### Personal Data Directly Accessible by the Candidate

- Personal data provided by the candidate as part of the Basic Information and Candidate Profile steps of the profile creation process can be accessed by the candidate without the need to submit a request. These fields are available for viewing when logged in.
- If data is captured on an iForm, through screening questions, or a configuration change makes the data unavailable, the candidate will have to submit a request to access this data (discussed in the section below).
- Access to personal data that is added to the candidate profile by recruiters will typically need to be requested.

### Personal Data Not Directly Accessible by the Candidate

- For any personal data not available for review in the candidate profile as described above (e.g., information entered by a recruiter or otherwise not provided as part of the Basic Information and Candidate Profile steps of the profile creation process by the candidate), there is a page accessible via the candidate dashboard that allows candidates to submit a request for access to any additional personal data.
- The candidate may enter an optional message with additional details as part of the request submission.
- Requests from candidates are visible in the customer system within a personal data request report. This report has a pre-configured templates, which can be modified as needed. The customer may enable a scheduled report to be emailed to a person from the customer's organization for review and processing.
- The iCIMS Talent Platform allows a customer to easily aggregate all the personal data for a given candidate. This can include screening responses, completed iForm, attached files, and data contained in fields. This feature includes configurations that allow the customer to

determine the data on the candidate profile that is in scope. This data will be downloadable as a .zip file which can contain common formats such as .pdf, .doc, .csv, etc.

- The customer will provide the requested information directly to the candidate.
- Based on the information above, the customer should ensure appropriate processes are in place to comply with data access requests.

## Right to Rectification/Correction

### For Personal Data Entered by the Candidate

- Most of the personal data provided by the candidate can be modified by the candidate without the need to submit a request. The fields that are part of the Basic Information and Candidate Profile steps of the profile creation process are available for updating when logged in.
- If data is captured on an iForm or through screening questions, or a configuration change makes the data unavailable, the candidate will have to submit a request to correct this data (discussed in the section below).

### For Personal Data Not Entered by the Candidate

- There is a page accessible via the candidate dashboard that allows the candidate to submit a request to have their personal data corrected.
- The candidate may enter an optional message with additional details as part of the request submission.
- The requests from candidates are visible in the customer system within a personal data request report. This report has pre-configured templates which can be modified as needed. The customer may set up a scheduled report to be emailed to a person from the customer's organization for review and processing.
- The customer will notify the candidate directly when the data correction is completed.
- Based on the information above, the customer should ensure appropriate processes are in place to comply with rectification/correction requests.

## Right to Portability

- There is a page accessible via the candidate dashboard that will allow the candidate to submit a request to be have their personal data delivered to them in a common file format.
- The candidate may enter an optional message with additional details as part of the request submission.
- The requests from candidates are visible in the customer system within a personal data request report. This report has pre-configured template that can be modified as needed. The customer may set up a scheduled report to be emailed to a person from the customer's organization for review and processing.
- The iCIMS Talent Platform allows a customer to easily aggregate all the personal data for a given candidate. This can include screening responses, completed iForm, attached files, and data contained in fields. This feature includes configurations that will allow the customer to determine what data on the candidate profile is in scope. This data will be downloadable as a .zip file which can contain common formats such as .pdf, .doc, .csv, etc.
- The customer will need to deliver the provided data to the candidate via email or another method.
- Based on the information above, the customer should ensure appropriate processes are in place to comply with portability requests.

## Right to Restriction of Processing

- There is a page accessible via the candidate dashboard that allows the candidate to submit a request to restrict the processing of their data.
- The candidate may enter an optional message with additional details as part of the request submission.
- The requests from candidates are visible in the customer system within a personal data request report. This report has pre-configured templates which can be modified as needed. The customer

may set up a scheduled report to be emailed to a person from the customer's organization for review and processing.

- Upon confirmation, and based on the customer's determination of alignment with GDPR requirements, the customer may be required to cease processing the candidate's data.
- The customer will initiate communication with the candidate, if needed, to confirm restriction of processing and determine any corrective actions.
- Any necessary corrective action(s) will be carried out by the customer. iCIMS will support the customer where reasonable and possible.
- If the corrective action resolves the candidate's request, the candidate can agree to allow the customer to reinitiate their processing activities. The customer will need to ensure appropriate communications channels are in place to accomplish this.
- Based on the information above, the customer should ensure an appropriate process is in place to comply with restriction of processing requests.

### Right to Object

- The candidate must contact the customer directly to object to any decisions made by the customer regarding personal data.
- When the candidate submits a request to address a data subject right via the portal, the customer should initiate communication (e.g., email, etc.) with the candidate to address the inquiry. Should the candidate wish to exercise their right to object to any decisions made, the objection should be provided by the candidate via an appropriate channel of communication determined by the customer. No capability is provided within the portal to initiate or provide communications capabilities around a candidate's right to object.
- Based on the information above, the customer should ensure an appropriate process is in place to comply with objection requests.

## Additional Information and Releases

iCIMS has a number of GDPR-related resources available on the iCIMS GDPR page: www.care.icims.com/s/gdpr-updates. Among other information, this page provides links to release notes that enable iCIMS customers to learn more about the system enhancements made so far in 2018 that further support iCIMS customers in their compliance efforts. Visit www.gdpr-info.eu for more information on the GDPR and other EU data protection developments.

iCIMS Talent Platform capabilities have been designed to allow customers sufficient flexibility and control regarding how they choose to implement their controller requirements. iCIMS will continue to study the evolving regulatory guidance and customer preferences, and may provide further capabilities, including increased automation, in future releases.