GDPR Tools for Companies

SmartRecruiters is committed to helping our customers ensure compliance with local compliance regulations. Our GDPR compliance tools provide the ability to manage candidates’ personal information and consent to the use of that information for recruiting purposes.

Introduction

SmartRecruiters’ GDPR tools helps companies to:

- Setup their Compliance configurations to manage candidate profile deletion and privacy policy wording.
- Create default and country level configurations for data retention, privacy policy and GDPR settings
- Obtain and manage candidate consent status
- Rules to manage automatic deletion of candidate profile based on the configurations setup above

SmartRecruiters also helps companies ensure compliance by providing candidates with the tools to manage their applications, personal information and consent.
Setting up Compliance Configurations

Under “Settings > Administration > Global Compliance”, you can setup your default compliance settings where you can control:

**Candidate’s right of data erasure**

How you would like to manage a candidate initiated request to delete their profile.

- Candidates can delete themselves automatically in Candidate Portal - no review needed.
- Candidates can request erasure in Candidate Portal - the administrator reviews the request and delete this candidate manually.

The second option (where the administrator reviews the request) requires that the candidate has job application(s). For instance a candidate who only has a community application - via filling out a lead capture form - will not be able to request erasure.
Privacy Policy Sentence

The wording you would like to use when your privacy policy is displayed at the end of a job application.

Privacy Policy Sentence

In case you have a privacy policy configured below, you can choose which sentence is displayed at the end of the application process:

- By checking this box, you will declare that you read and understand Acme Corp. 091614’s privacy policy.

- By checking this box, you will declare that you read and agree to Acme Corp. 091614’s privacy policy.

Please note if you are using CRM, the change is not yet propagated in Lead Capture Forms.
Default and Country level policy settings

You can make changes to the below fields in your Global Compliance settings:

1. **Data Retention**: how you would like to treat candidates that have either been rejected, withdrawn, removed from the job or hired

2. **Privacy Policy**: adding a URL link of your company privacy policy

3. **GDPR settings**: toggle to remove candidate's application if they do not provide consent within 30 days.

By default, SmartRecruiters adds a default configuration ruleset to your account, and will apply these default compliance rules to jobs in **any country for which you don't set up a specific configuration**.

You can also add country-specific configurations with differing privacy policies and data retention periods.
SmartRecruiters will use a job's location to determine which configuration applies to that job.

- If you post jobs in only one country, either modify the default configuration, or just set up a new configuration for that specific country.
- If you post jobs in more than one country, it's a good idea to set up a configuration for each country.

Kindly note that any changes to the GDPR settings does not retroactively apply to consents that have been sent to candidates. Please ensure you take the necessary steps to manages candidates accordingly based on the changes made.

https://help.smartrecruiters.com/GDPR/GDPR_Tools_for_Companies

Updated: Thu, 16 Jul 2020 05:31:46 GMT
Obtaining candidate consent

There are four ways for you to obtain consent from your candidates:

1. **Default or country level privacy policy settings**
   
   (under "Settings > Administration > Global Compliance"). Once setup, all Candidates who apply to a SmartRecruiters job ad will see a check box at the bottom to review and consent to your privacy policy.

   **Default, when nothing is configured**

   - Please be informed that your application to this job offer will trigger some processing of your personal data by the recruiting company, the data controller. SmartRecruiters, the data processor, has no control over such personal data processing. For more information on these personal data processing, please refer to the recruiting company's privacy policy.

2. **Recruiter uploads a resume of a candidate into the system**

   System identifies if candidate already exists in the system. If yes, it will pick up the same consent status as the existing candidate profile

   If consent is missing, the recruiter will need to send the consent to the candidate either manually via the SmartRecruiter platform (details below under managing candidate consent).

   Please see the SmartRecruiters default template that the candidate will receive below:
For jobs with GDPR settings turned off:

Hi [Candidate First Name] [Candidate Last Name],

We’d like to consider you for employment at [Company name]. Your privacy is important to us, so please review our privacy policy and confirm that we may use your information for recruiting purposes.

[Review policy]

You can view, update, or delete your profile at any time.

Thank you,

[Company] Recruiting Team

For jobs with GDPR settings turned on:

Hi [Candidate First Name] [Candidate Last Name],

We’d like to consider you for employment at [Company name]. Your privacy is important to us, so please review our privacy policy and confirm that we may use your information for recruiting purposes. If you do nothing, your profile will be deleted in 30 days.

[Review policy]

You can view, update, or delete your profile at any time.

Thank you,

[Company] Recruiting Team

These templates are configurable under “Settings > Templates > Custom Consent Request”

3. Employee refers a candidate to a job in your company

Referrer is asked to confirm that they have permission from the candidate to submit their information prior to submitting a referral.

I hereby confirm that I have received the authorization to forward the above mentioned information from the referral *

MAKE REFERRAL

Once the referral is made, the candidate is added in the Lead status to a job, and will receive the following email:
For jobs with GDPR settings **turned off**:

Dear [Referral First Name] [Referral Last Name],

[Referrer First Name Referrer Last Name] referred you to the position of [JobTitle] in [JobLocation] at [Company]. If you're interested in the position, you can apply by viewing the job ad here [link] and clicking "I'm Interested".

Thank you,

[Company] Hiring Team

For jobs with GDPR settings **turned on**:

Dear [Referral First Name] [Referral Last Name],

[Referrer First Name Referrer Last Name] referred you to the position of [JobTitle] in [JobLocation] at [Company]. If you're interested in the position, you can apply by viewing the job ad here [link] and clicking "I'm Interested". *If you do not, your information will be deleted from [Company] in 30 days.*

Thank you,

[Company] Hiring Team

4. Application API

Companies and partners who have built a custom application experience using our Application API should ensure that they present candidates with the appropriate privacy policies and collect the candidate’s consent. Make sure to specify the candidate’s consent by setting the `consent` property to `true` in a POST request to the `/postings/:uuid/candidates` endpoint. The property is `false` by default.

Kindly note the retention period of each application is based on the GDPR setting used at the time the consent is sent.

For example, if the GDPR setting is **turned on** when the consent is sent to the candidate, the candidate profile will still be deleted after the retention period if no consent is obtained even if the GDPR setting was changed to **off** within that period.
Managing Outstanding Candidate Consents

Consent is stored on the candidate profile. Recruiters can check the candidate’s profile to verify whether they’ve provided consent for the use of their application.

Candidates who’ve applied numerous times, to different jobs at your company, will provide consent on each application. You’ll be able to see the date for the most recent record of collected consent.

Candidates can withdraw this consent from a particular company at any time.

Anyone with the permission to do so (as defined in the custom hiring team roles) can request consent by clicking “Request Consent” on the candidate’s profile, triggering an email to be sent to the candidate.

It’s important to remember that consent is associated with a candidate’s profile, not their applications. If the candidate has already consented, there’s no need to re-request consent when adding the candidate to another job.
Managing Candidate Response

If the candidate accepts the consent request, this sets the date of the latest consent on their profile. This consent date is visible to users with access to any of the applications of this candidate.

For jobs with GDPR setting turned on, if the candidate does not respond OR declines to grant consent within 30 days from the consent request date, their data, including all applications associated with that candidate, will be removed - regardless of whether they had previously provided consent.

When a candidate’s application is deleted, the system sends notifications to the Recruiters assigned to the hiring teams of the roles where the candidate had an application. If there are no Recruiters then emails are not sent.

Find out more on the process of Automatically Removing Candidate Data.