EVERYTHING YOU NEED TO KNOW ABOUT
PHENOM & GDPR

phenom

GDPR
What you need to know

In 2016, the European Union (EU) adopted the General Data Protection Regulation (GDPR) — one of the most important changes in data privacy regulation in decades. The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, protect and empower all EU citizens' data privacy, and reshape the way organizations across the region approach data privacy.

The purpose of GDPR is to create and enforce uniform data protection regulations, so each member state no longer has to write its own data protection laws while creating consistent data privacy laws that apply to the entire EU.

Who does GDPR affect?

Now recognized as law across the EU, this regulation is the baseline for data privacy in the EU. However, all 27 member states that make up the EU are at liberty to fine-tune to their specific requirements for data protection and privacy.

The GDPR not only applies to organizations located within the EU — it also applies to organizations located outside of the EU if they offer goods or services or monitor the behavior of EU data subjects. GDPR applies to all companies processing and holding the personal data of data subjects residing in the EU, regardless of the company's location. It also requires that companies have a lawful basis in order to process personal data.

What are the penalties for non-compliance?

Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million. This is the maximum fine that can be imposed for the most serious infringements (e.g., not having enough customer consent to process data).

phenom

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Phenom.

2

KEY
DEFINITIONS

Data subject

An individual who can be reasonably identified, directly or indirectly, by processing their personal data

Personal data

Any information relating to an individual who can be identified directly or indirectly by use of personal data — that could be combined with other data — which in turn would make an individual reasonably identifiable

Controller

The entity that determines the purposes, conditions, and means of processing personal data

Processor

An entity which processes personal data on behalf of the controller

Data breach

A breach of security that leads to the accidental, unauthorized, or unlawful loss, disclosure of, or access to personal data processed

Transfer

Any movement of data or viewing of data outside of the EU

MAINTAINING GDPR COMPLIANCE

with Phenom

4

Phenom is fully committed to helping our customers meet GDPR compliance obligations. This document to highlight:

- **GDPR guidelines that are relevant to career sites**

- **The approach Phenom has adopted for GDPR in its role as the data processor**

- **Workflows that will be provided to our customers to meet their responsibilities as a data controller**

Both Phenom and our customers have shared responsibilities towards ensuring compliance — our customers are **data controllers** and Phenom is a **data processor** because we are acting on behalf of the client. Phenom is only a processor for the activities that we directly carry out for the performance of the service on behalf of the customer (e.g., setup, architecture, and data flow).

Data Subjects

Your prospects and candidates are the data subjects. It is their personal data that is processed when they are considered for a position or kept in a talent pool.

Data Controller

You are the data controller and can determine the purpose and usage of the data directly related to your service.

Data Processor

Phenom is your data processor. Our platform maintains and protects your candidates' data.

DATA
PROCESSING

There are several available lawful bases for data processing — one way to stay compliant is by obtaining the user's consent. Consent means offering users the real choice and control through an opt-in/opt-out mechanism.

With respect to career sites, Phenom has adopted a user content-based approach for candidate tracking and personalization features.

Even if your career site might list jobs for locations strictly outside of the EU, candidates from the EU can visit the career site and provide their personal information. Phenom's approach aims to secure and safeguard data privacy for all candidates that visit the career site, which means the scope of this implementation applies to all customers.

phenom

What Data Elements
DOES PHENOM PROCESS?

Phenom Talent Experience Management (TXM) is a single SaaS platform hosted on AWS cloud with a multi-tenant architecture — meaning all clients are included in the same code base, but each set of data is segregated using unique client reference numbers (refNUM). Each unique reference number is assigned to a dedicated database schema and separated by endpoint URLs.

Phenom may store a candidate's CV, resume, or job application data, and what's minimally required to create a profile or submit a job application within a CRM. This information includes:

- **First Name**
- **Last Name**
- **Email**
- **Phone Number**
- **Address (optional)**

Phenom only collects data required for the performance of the service to its customers. Customers may request Phenom to process additional or different types of personal data beyond what Phenom requires for service performance. This remains the sole responsibility of the Customer as Data Controller. Phenom as Data Processor does not determine the purpose or means of personal data with respect to the Data Controller.

Out of the box, Phenom only captures and stores limited personal data that can easily change depending on what the Data Controller instructs the Data Processor to capture. It is the Customer's responsibility to have controls and processes in place to ensure that only the necessary personal data is requested to be captured by Phenom.

phenom

Basis for the Processing of
PERSONAL INFORMATION

GDPR requires that companies should have a lawful basis in order to process personal data. There are several available lawful bases for processing. One of these is by obtaining the user's consent. Consent means offering users the real choice and control through an opt-in/opt-out mechanism. With respect to career sites, Phenom has adopted a user consent-based approach for candidate tracking and personalization features.

1 COOKIE CONSENT BANNER
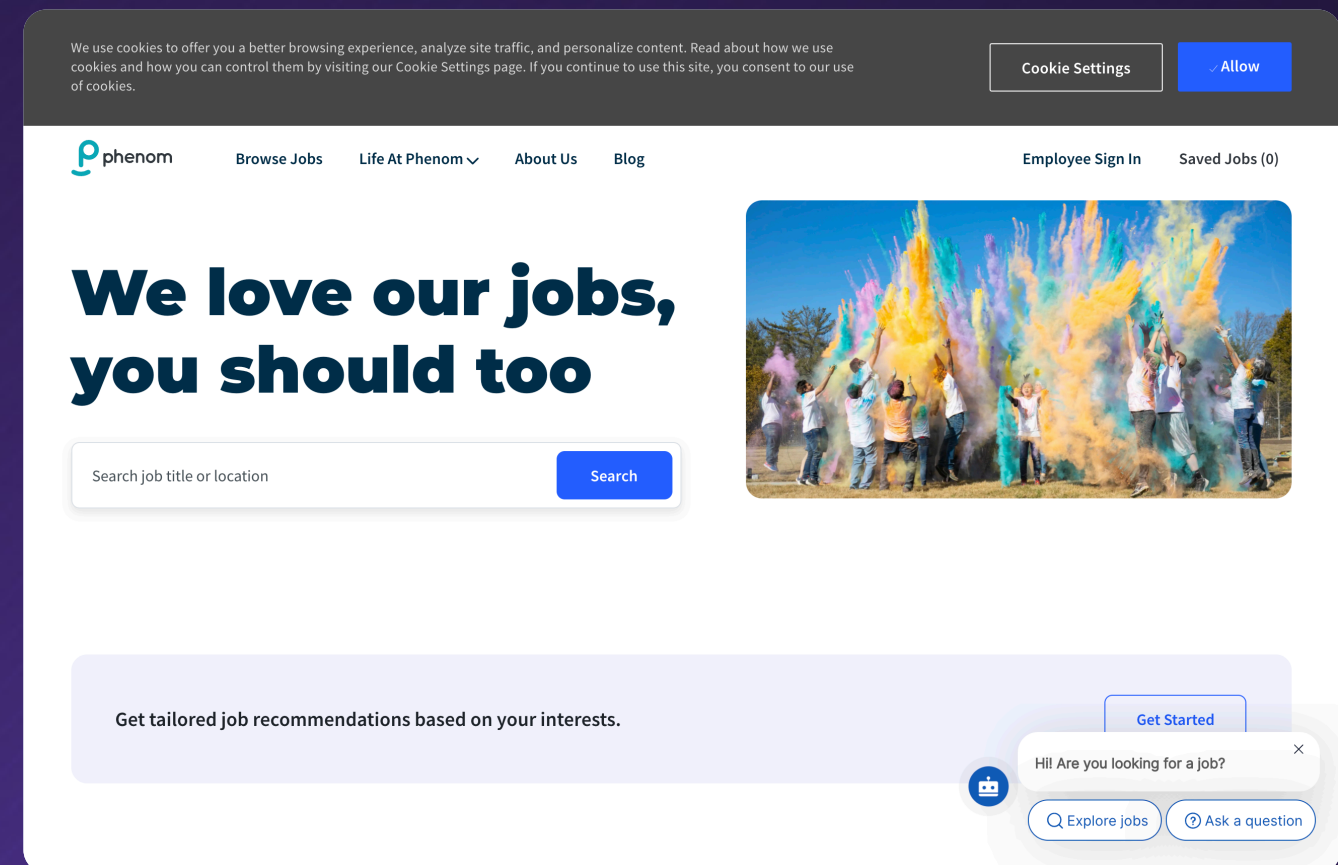## to accept or decline tracking

Feature functionality:

On the Phenom career site, a cookie consent banner will pop up when a candidate visits the career site. This will prompt the user for consent to track their activity (see screenshot example).

Candidate activity tracking allows Phenom to provide personalized job recommendations on the career site based on their browsing behavior. The candidate can decline tracking on the cookie settings page by clicking on the cookie setting button on the banner and unchecking performance and personalization cookies option.

Phenom also offers the cookie consent to appear as a cookie pop up upon request.

The cookie banner is the preferred option.

phenom

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Phenom.

9

CANDIDATE
Experience

When a candidate visits the career site for the first time, they're presented with a cookie consent banner (as shown in the screenshot above). The candidate can either accept, decline (from the cookie setting page), or ignore cookie consent:

If the candidate accepts cookie consent, the candidate activity is tracked on the Phenom platform.

If a candidate ignores the cookie consent, the candidate data is not tracked.
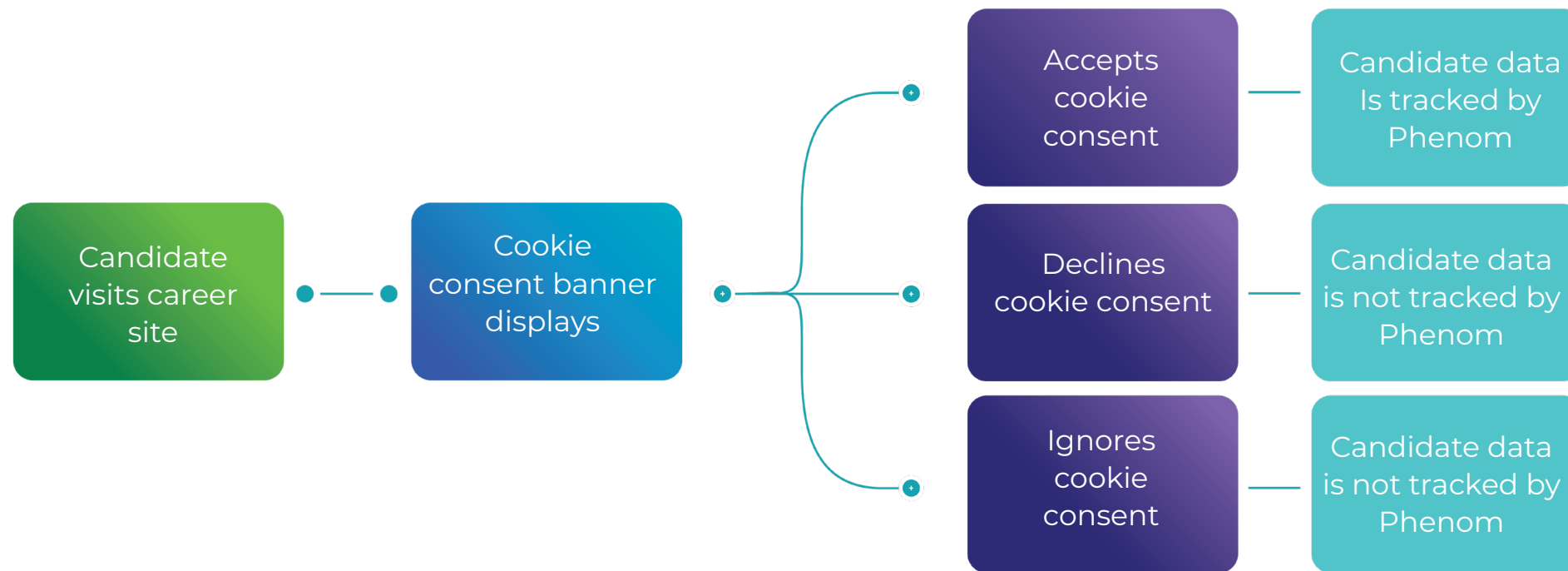
If the candidate declines the cookie consent, the candidate activity is not tracked on the Phenom platform. Candidates can decline cookie consent on the career site cookie settings page that is linked to the cookie settings option on the banner.

The cookie consent banner will remain on the screen until a user provides an input.
On subsequent visits to the career site, the candidate's previous selection will be remembered.

- Cookie consent is specific to a browser. So if a candidate declines cookie tracking on Google Chrome and then visits the career site on Safari, the consent banner will be shown to the candidate again.

- The consent checkbox across the career site is a configurable feature that the client would request during implementation.

Candidate visits career site → Cookie consent banner displays →

Accepts cookie consent — Candidate data Is tracked by Phenom

Declines cookie consent — Candidate data is not tracked by Phenom

Ignores cookie consent — Candidate data is not tracked by Phenom

phenom

2 CAREER SITE COOKIE POLICY
pre-footer section

Feature functionality:

At any time, the candidate should have the ability to change their cookie consent decision. To facilitate this, a new section called the pre-footer will show up on the career site that lies above the footer section.

The pre-footer contains a link to the career site cookie settings page.

The career site cookie setting page provides options for the candidate to toggle cookie consent. This page highlights the following cookie categories:

- Essential cookies that are strictly necessary for proper functioning of the career site. The user cannot disable this.

- Personalization and performance cookies track user activity and provide a personalized experience to candidates visiting the career site. The candidate has the ability to turn off cookies and decline tracking.

If you decline consent to cookies, you may still use this career site, but your ability to use some areas of limited. For example, you cannot receive job recommendations on this career site based on your browsi career site will not be able to personalize your experience. You will still be able to apply for jobs through application forms, log in to this career site using LinkedIn, join the Talent Community or subscribe to Si

How can I control cookies?
Personalization and Performance cookies can be controlled by checking or unchecking your consent on Overall, you are able to control cookies from your browser-level settings. Each browser typically allows disable, block, allow, or remove cookies by visiting the settings, tools, or preferences tab that can be lo browser itself. For additional questions regarding any specific browser, please contact your browser sup

Career Site Cookie Settings

phenom

300 Brookside Ave
Building 18 Suite 200
Ambler, PA 19002

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Phenom.
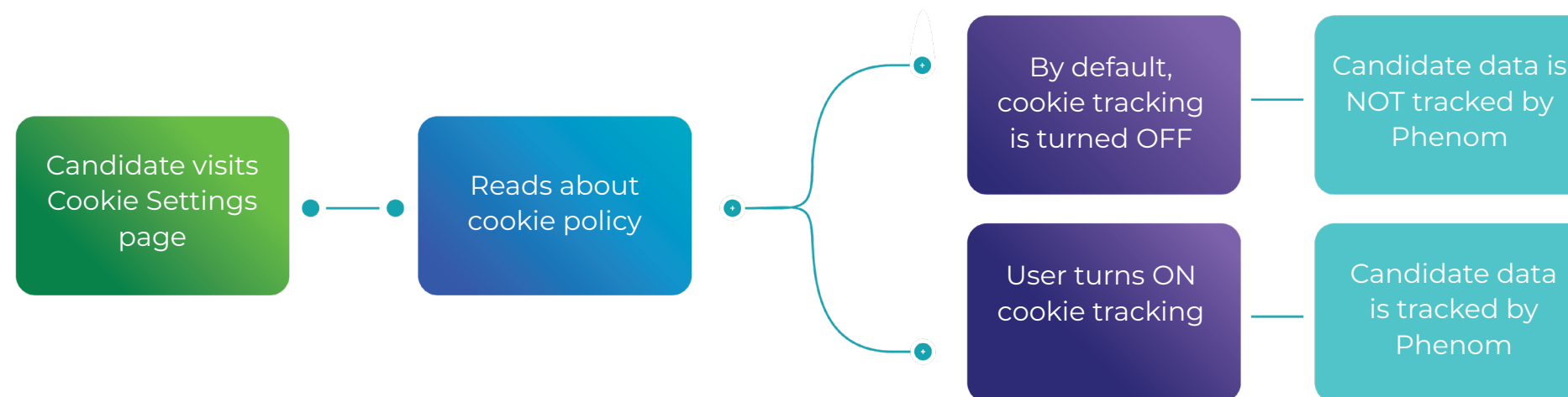
12

CANDIDATE
Experience

When the candidate visits a career site and scrolls down to the pre-footer, they will see a link to the Career Site Cookie Settings page. Clicking on this link will bring them to the page where they can view cookie policy details and manage their personalization and performance cookies by turning consent on or off. They can access this page and make changes at any time.

All candidate activity related to cookie consent is handled on the candidate's browser. The customer (data controller) does not need to take any processing action for this activity.

```
Candidate visits
Cookie Settings
page
```
→
```
Reads about
cookie policy
```
→
```
By default,
cookie tracking
is turned OFF
```
→
```
Candidate data is
NOT tracked by
Phenom
```

```
User turns ON
cookie tracking
```
→
```
Candidate data
is tracked by
Phenom
```

TYPES OF COOKIES

Essential cookies are automatically added onto the user's computer or device when they access a customer's career site. **Non-essential** cookies are added only when the user has provided consent.

To deliver personalized experiences, Phenom uses the following essential and non-essential cookies to track and monitor user behavior:

phenom

ESSENTIAL COOKIES

Cookie Name	Data Elements	Cookie Type	Expiration	
in_ref	Initial Referrer: Original souce of traffic to the career site	Session	Session	Essential
utm_source	Identify the advertiser, site, publication, etc.	Session	Session	Essential
utm_medium	The advertising or marketing medium	Session	Session	Essential
utm_campaign	The individual campaign name	Session	Session	Essential
utm_content	Used to differentiate similar content, or links within the same ad	Session	Session	Essential
utm_term	Keyword to identity campaign	Session	Session	Essential
VISITED_LANG	Career site language (EN, FR)	Persistent	365 days	Essential
VISITED_COUNTRY	Visited from Country (IN, UK)	Persistent	365 days	Essential
VISITED_VARIANT	Visited Site type or persona (student/professional)	Persistent	365 days	Essential
jwtToken	Used for login session management	Persistent	30 days	Essential
JSESSIONID	Used for session management	Session	Session	Essential
PHPPPE_GCC	Tracks if the user has declined cookie tracking on the cookie banner/settings page	Persistent	90 days	Essential
PHPPPE_NPS	Tracks if the user has seen NPS feedback popup or not, its optional feature	Session	Session	Essential
PHPPPE_EXINT	Tracks if the user has seen exit intent pop-up or not, optional feature	Session	Session	Essential
PHPPPE_CVD	Tracks if the user has accepted/declined the COVID banner	Session	Session	Essential
PLAY_SESSION	Used to prevent malicious actors from tampering with a user's session	Session	Session	Essential
JSESSIONID	Used for session management with SSO	Session	Session	Essential
route	Used for maintaining the routing info	Session	Session	Essential
ext_trk	External Apply Tracking Parameters	Session	Session	Essential (if an apply redirection is in place)

NON-ESSENTIAL COOKIES

Cookie Name	Data Elements	Cookie Type	Expiration	
Per_UniqueID	System generated unique identifier for browser thumbprint	Persistent	365 days	Non-essential
gclid	globally unique tracking parameter (Google Click Identifier) [DEPRECATED]	Session	Session	Non-essential
P_REF_CNG	Flag to avoid wrong referral while login with social accounts	Session	Session	Non-essential
overlayDismissed	Cookie banner Accept/Cookie Settings (prior to GDPR)	Persistent	Session	Non-essential
PHPPPE_STID	Track unique login session in case of multi-user on same browser	Persistent	30 days	Non-essential

phenom

RIGHT TO ACCESS, DATA PORTABILITY, AND ERASURE

GDPR provides certain rights to data subjects. Here are a few rights that are relevant to Phenom customers' career sites:

- Right to access:
  Data subjects have the right to access their personal data and supplementary information stored in the system (Article 15).

- Right to data portability:
  Data subjects have the right to obtain, copy, and re-use their personal data for any purpose (Article 20).

- Right to erasure:
  Data subjects have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This is also known as "the right to be forgotten" (Article 17).

To maintain GDPR compliance, the Phenom platform offers all of the rights above to candidates who visit a career site.

1 PERSONAL INFORMATION SECTION
and request workflow

Feature functionality:

Within the pre-footer on the career site, there is a link to the "Personal Information" page, which provides details about the type of personal information that is stored by the career site. It also outlines how a candidate can request to view or delete any personal information.

phenom

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Phenom.

17
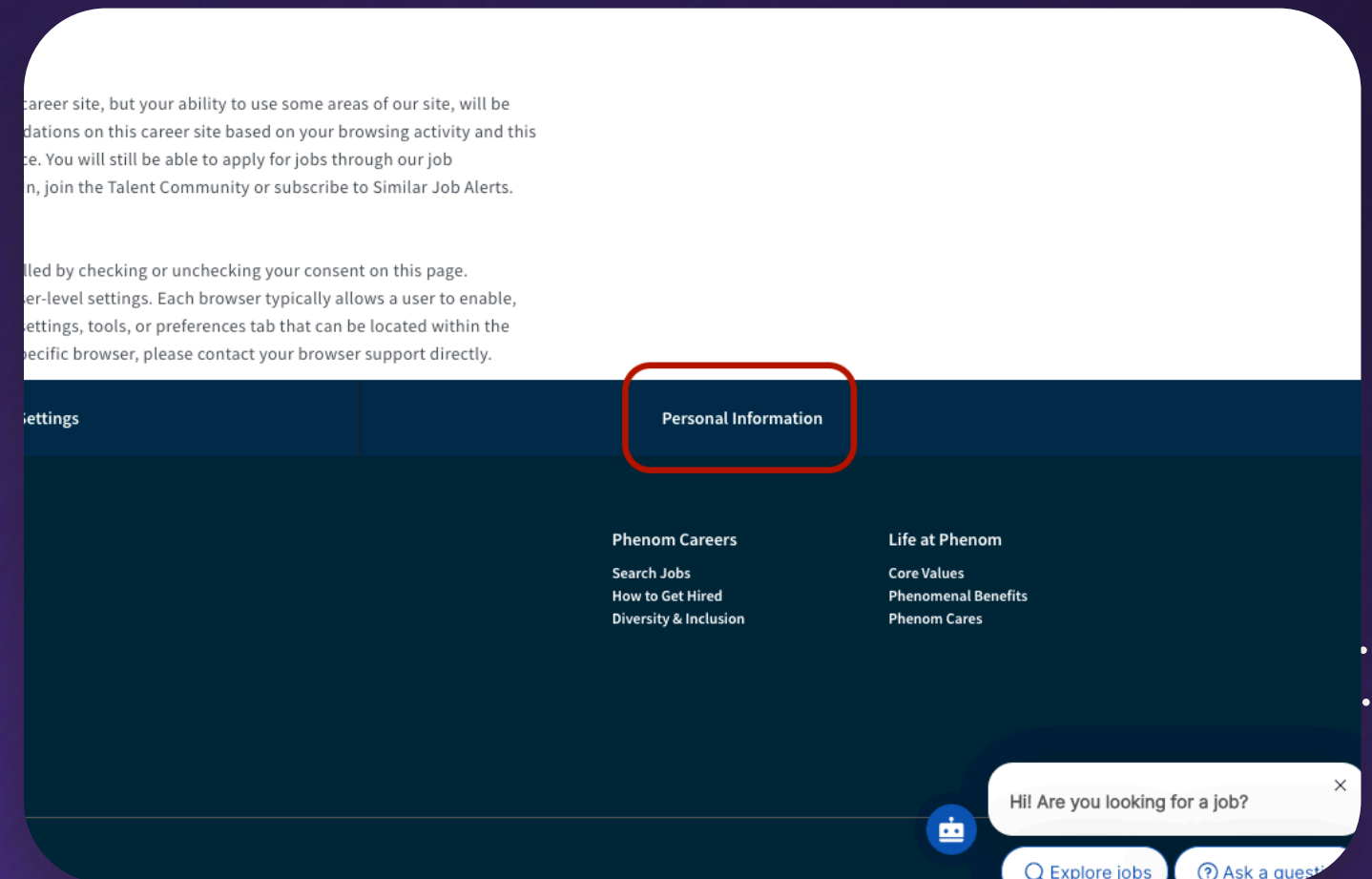
CANDIDATE
Experience

A candidate who visits a career site can access the link to the "Personal Information" page in the prefooter. From here, they can submit a request to view, download, and/or delete their personal information.

Candidates will receive an email to verify their email address in order to complete the request.

ABOUT PERSONAL INFORMATION

Career site stores your profile information when you log-in to the career site using LinkedIn, apply for jobs, subscribe to job alerts or join Talent communities.

This page provides a mechanism for you to submit a request to view or delete your personal information stored on the career site. You are required to provide your email and complete email verification in order to submit this request. Any requests will be reviewed and responded within 30 days.

Please be aware that requesting a deletion of personal information will remove your entire profile information from the career site including any active job applications. This will also remove any subscriptions you might have made on the career site.

Manage Personal Information
Request to view, download and delete your personal information
This workflow applies to EU data subjects only

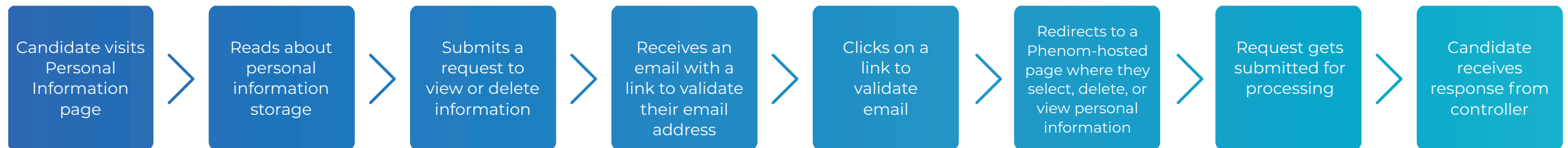Career Site Cookie Settings   Personal Information

phenom

300 Brookside Ave
Building 18 Suite 200

Phenom Careers   Life a

Search Jobs   Core
How to Get Hired   Ph

CANDIDATE
Experience

After verifying their email by clicking the link, the candidate will be able to either view or download their personal information, as well as request to delete their profile from the career site page. The diagram below shows the overview of the entire workflow.

Candidate visits Personal Information page → Reads about personal information storage → Submits a request to view or delete information → Receives an email with a link to validate their email address → Clicks on a link to validate email → Redirects to a Phenom-hosted page where they select, delete, or view personal information → Request gets submitted for processing → Candidate receives response from controller

THE CUSTOMER (data controller)
Experience

When a candidate submits a request to view or delete their personal information, the request is logged on the Phenom platform.

Once a day, the Phenom platform will notify the customer via email about any new view/delete requests it received from candidates on the career site. The email will contain the total number of requests received by candidates, as well as a breakdown of total view requests and deletion requests.

This notification will be sent to a designated email inbox that the customer provides to Phenom for processing GDPR requests during onboarding. The email will not be sent if no candidates make any requests.

The email will also include a link that allows the customer (data controller) to log in to the Phenom platform to view and authorize the requests.

phenom

Hello,

You have 5 profile processing requests from candidates from your career site:

- 4 View profile requests

- 1 Delete Profile Information request

View and authorize these requests by logging into **Phenom's CRM platform.**

Thank you

Phenom GDPR Privacy team

phenom

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Phenom.

20

Once logged in to the Phenom platform, authorized administrators (provisioned during GDPR onboarding) will see a menu called "Privacy" that shows all candidate requests for processing personal information.

The customer will need to take action to authorize Phenom as a data processor to process some or all requests. Customers will also have the ability to export requests as a CSV file.

Once the requests are authorized, Phenom will process these requests and track their status.

Note: For any deletion requests, all personal information of the candidate, including applications, are deleted from the Phenom platform in 24 to 48 hours. Once the process is complete, the email address that was used as part of the request will also be deleted. As a result, we recommend downloading the request report to a CSV format for tracking and authoring before authorizing requests.
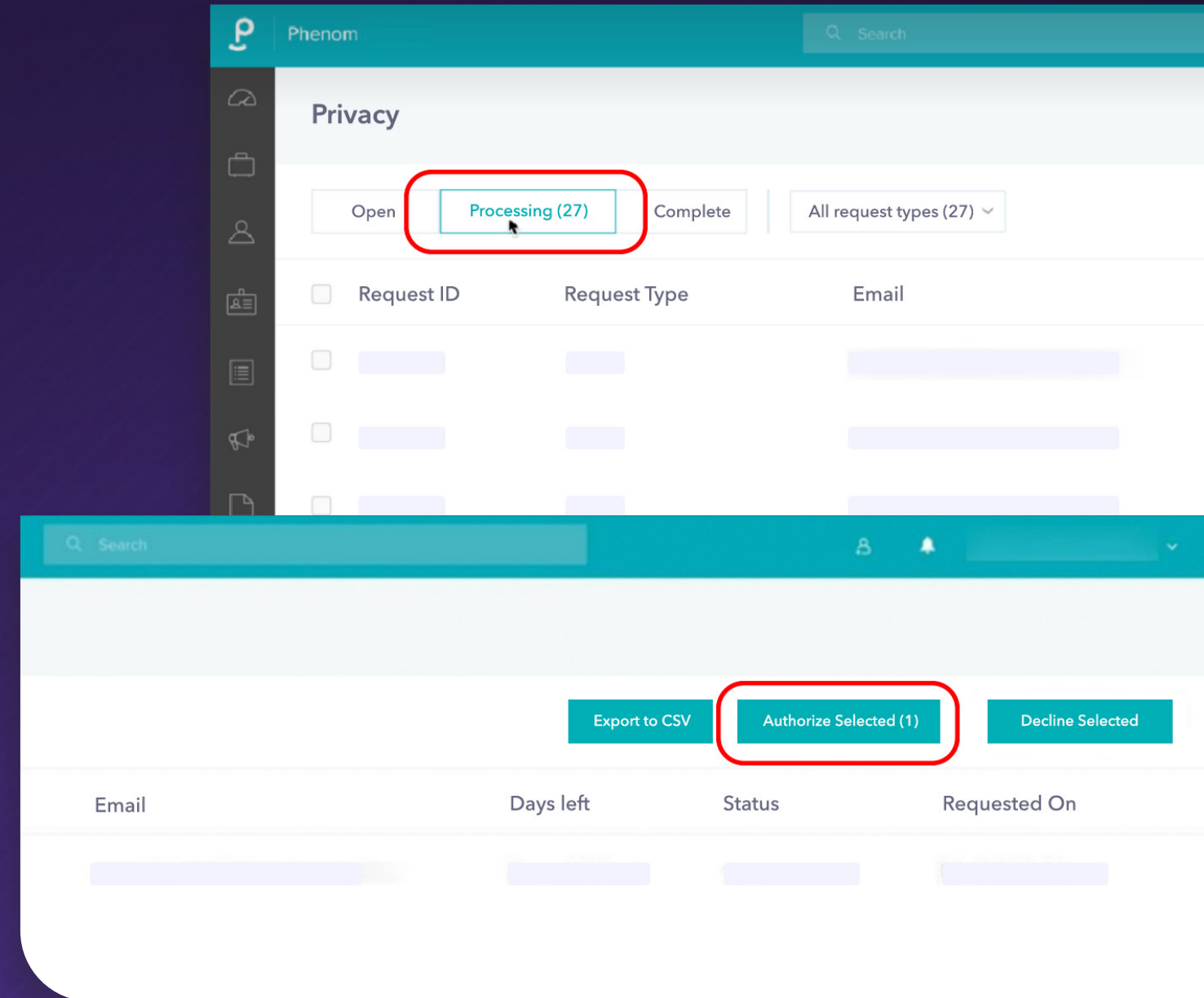
An email confirmation will be sent to the customer's registered email inbox notifying the completion of the request. Customers can log in to the Phenom platform to view the status.

For requests to view data, customers can download personal information profiles that were processed by Phenom. The customer is expected to also submit this request to other processing systems where candidate data might be stored, such as an ATS, HRIS, etc.
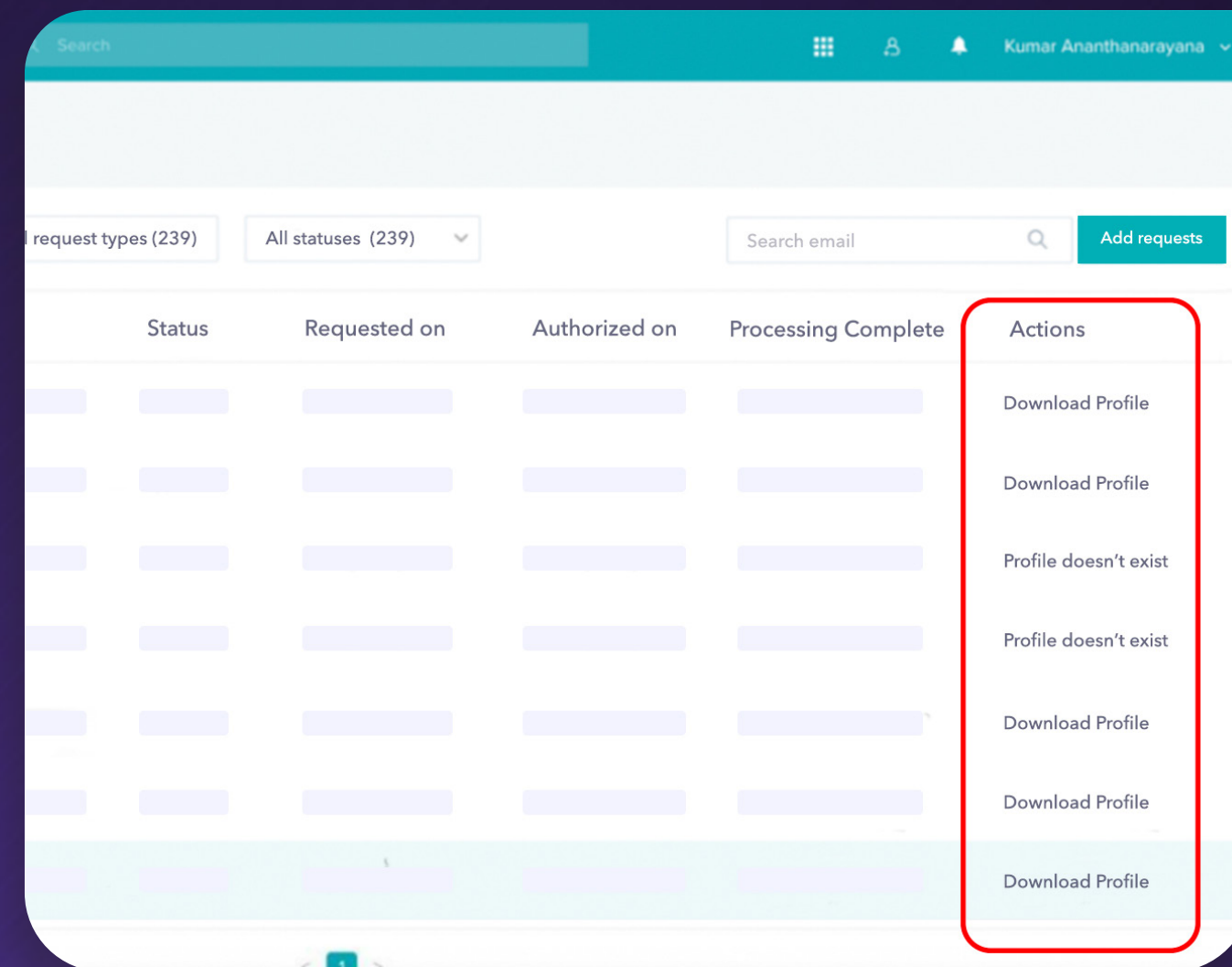
Once the responses have been collected from all systems, the customer will send a notification to the candidate with the requested personal information. Please note that it is the customer's responsibility to inform the candidate of any updates.

This workflow explains the process for viewing, downloading, and deleting information:

| Candidate submits request to view or delete infomation | → | Career site validates candidate's email address | → | Customer is notified about the request via email | → | Customer authorizes Phenom to process the request | → | Phenom processes the request | → | Customer processes the request from other internal | → | Customer notifies candidate on successful completion |

2 DELETING CANDIDATES
from the CRM

Due to GDPR and other data privacy regulations, there is a need to remove candidate personal identifiable information (PII) from the Phenom platform either due to a candidate request or to be in compliance with data retention periods. Details for the removal of inactive or stale candidate data from the CRM are as follows.

phenom

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Phenom.

24

PURGING
Applicant data

For customers using Phenom as the experience layer for their ATS — where the ATS is serving as the system of record for applications — the request for data deletion should originate from the ATS. This can be accomplished via file feed to Phenom using the following steps:

Phenom will set up an SFTP site where the customer can upload a list of candidates

Customer will upload a list of candidate email addresses to be removed from the Phenom platform

Phenom will process the list, purge the candidate information from the system, delete the list, and provide a confirmation back to the customer

This process requires a custom integration. Any customers interested in setting up this process should speak to their Phenom Account Manager.

PURGING
Lead data

Phenom does not purge any data.

For candidate PII that only resides in the Phenom platform (either pre-apply or customers using Phenom quick apply), users (recruiters) can create a list within the CRM to delete information based on the data retention period.

If the privacy policy specifies a single retention period based on last activity of the candidate, the candidate list can be filtered based on "Candidate Last Activity Date" (see process here) and that list can be downloaded for use in purging other systems and uploaded via the GDPR Privacy workflow for bulk deletion (Note: the list must currently be downloaded, converted to CSV UTF-8 (comma delimited) file, and uploaded into the GDPR Bulk Delete workflow; we are actively working on a one-click deletion process to avoid this extra step).

Clients that require different data retention periods based on candidate location (e.g., six months for Germany, 24 months for France) can create different lists for each retention period, but will need a default list for candidates that don't have a location associated with them (e.g., candidates that sign up for a job alert provide an email address but aren't required to provide a location). The period for the default list should line up with the shortest retention period to avoid missing any candidates.

phenom

For example, to set up the list for the French retention period (24 months), navigate to the "Candidates" tab and click "Filter", then "Advanced Mode" at the bottom. Set the following parameters:
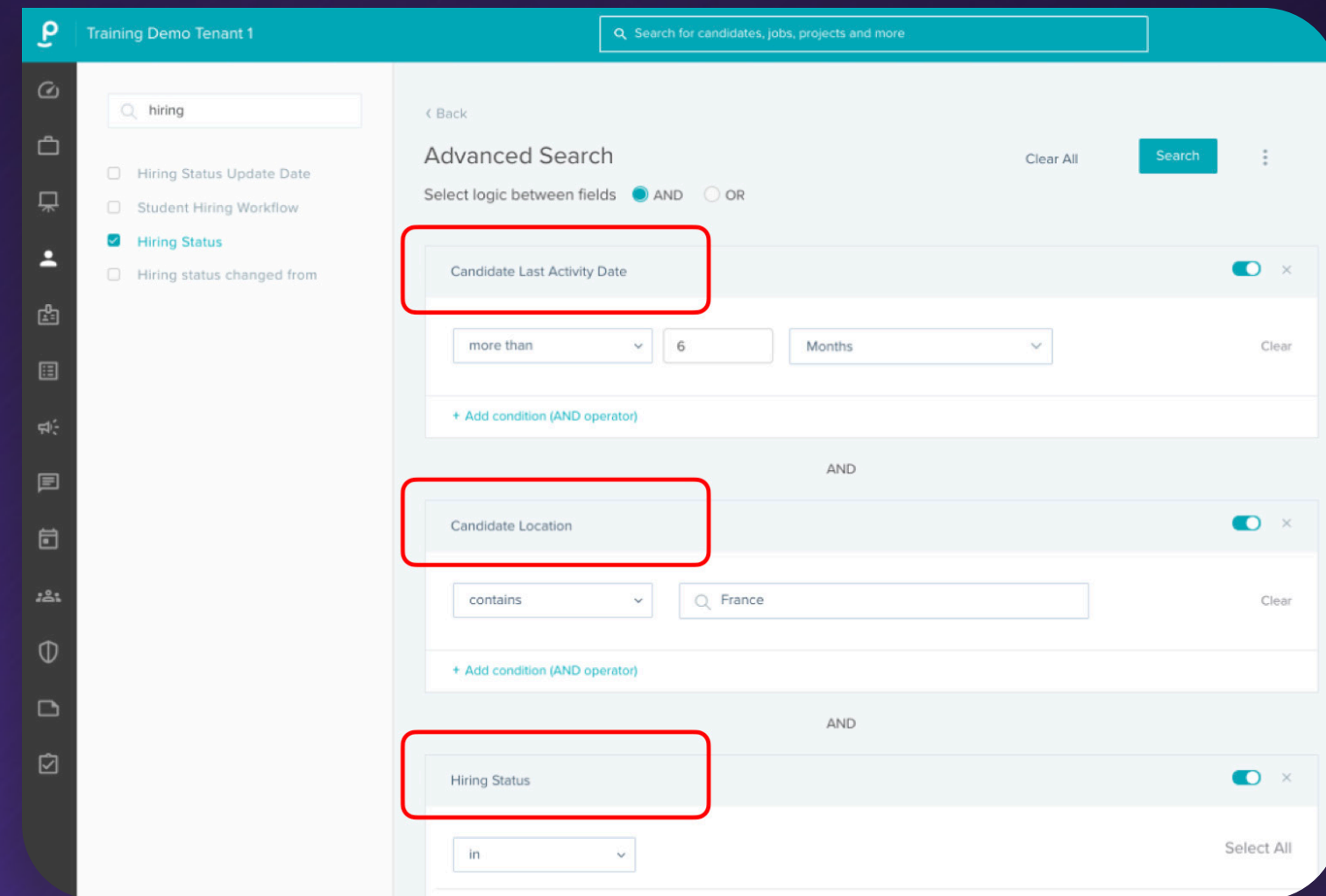
"Candidate Last Activity Date"
more than 24 months

"Candidate Location"
contains "France"

"Hiring Status" in Any CRM Lead
Status (varies by customer)

Once the criteria are set, click "Search". Once back on the "Candidates" tab, on the "Filters" box, click "Save", then "Create Dynamic List". This list can be automatically submitted for deletion on an as-needed basis. Navigate to the "Lists" tab, click on the specific list you want to delete, and choose "Delete".

Create your other retention period lists following the process above and changing the number of months as appropriate. As mentioned, be sure to create a default list for candidates without a location (set "Candidate Location" filter to "is empty") that is in line with the shortest retention period.

*Note: Deleting a list **does not** delete candidates within that list. You must select all candidates in a list and submit for deletion.*

AUDIT TRAILS

Any request that the customer authorizes Phenom to process will be audited. The audit history will contain the request details, the time when the request was made, and when the request was processed.

In the case of deletion requests, Phenom will not store the candidate's email address in the audit trail as deleted, since this will be considered personal information that was being requested for deletion.

ALTERNATE WORKFLOW

If the customer has their own GDPR solution in place, Phenom can configure the workflow to integrate with the customer's existing solution. The "Personal Information" link on the career site can be configured to redirect candidates to centralized GDPR request pages that customers may have, and allow candidates to submit requests through this process.

GDPR administrators can log in to the Phenom CRM to process any GDPR requests to view or delete candidate information by submitting the request using the "Add Request" workflow shown below.
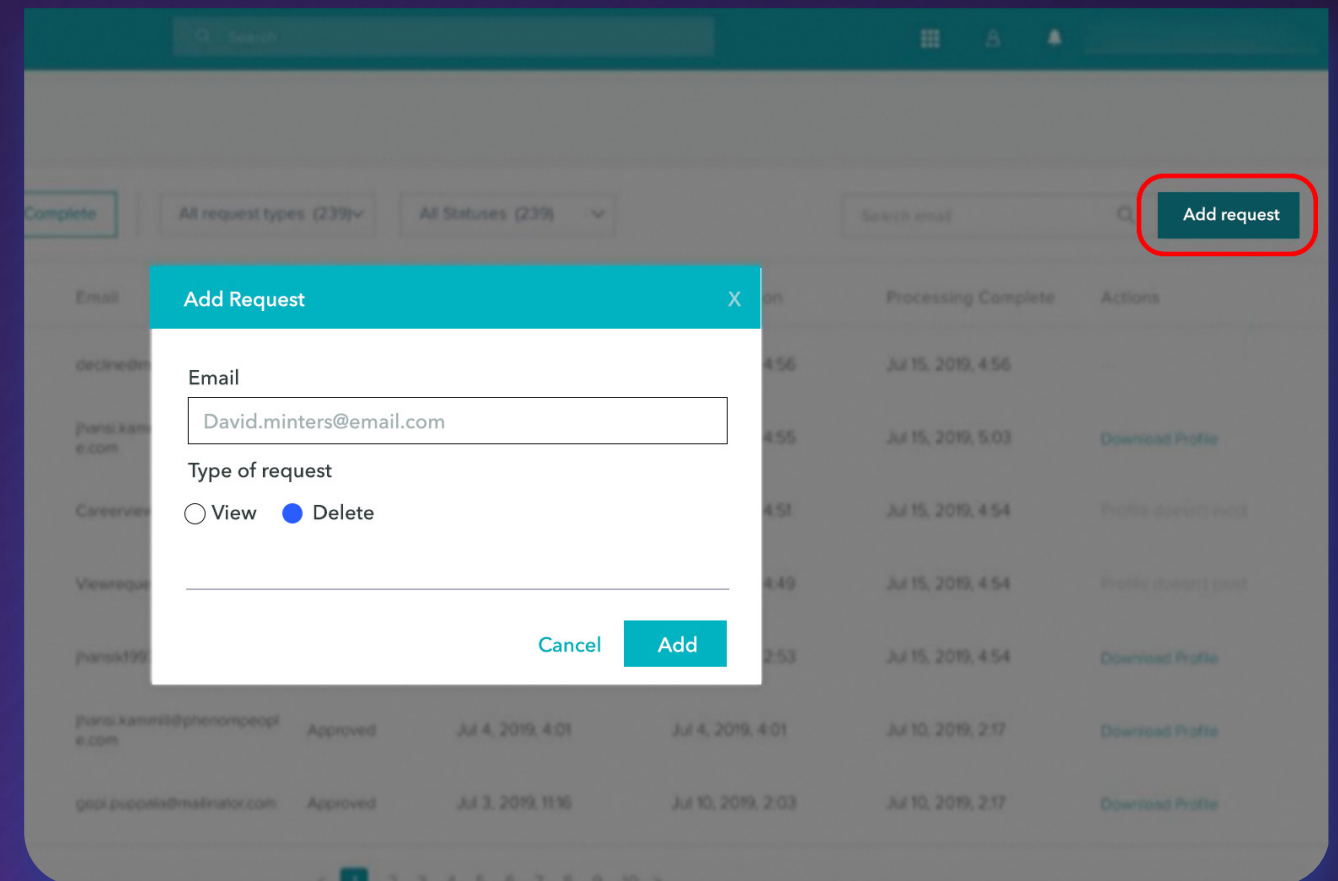
INTERNAL MOBILITY
Referral form: GDPR Consent

Customers have the option to add employee consent on the Internal Mobility Referral form for employees to indicate whether they have the consent of the person they're referring. Here is how it works:

Employee may select "Yes" or "No". Selecting "No" does not stop the referral process

Consent is sent to the CRM as part of the referral form answers

The consent is saved in the CRM as part of the candidate profile and is available under "Attachments"

phenom

DATA TRANSFER
& DATA HOSTING

The personal data relating to our EU and UK customers is located on our services in Ireland, and backup is also in Ireland. As a result, we may need to make certain personal data available to/accessible from jurisdictions located outside of the EU and the UK for limited, prescribed purposes.

After closely monitoring the legal developments to which we are subjected to when personal data is transferred outside of the EU or the UK — including the Schrems II ruling by the Court of Justice of the European Union and recommendations issued by the European Data Protection Board — we have taken steps to strengthen our internal measures and safeguards to protect data transferred outside the EU. This includes:

phenom

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Phenom.

32

Strict measures to regulate internal access to our customers' data. This is on a clearly defined role and needs basis, limited to task/time and frequently audited. In practice, aside from database administrators, only a select number of our employees located outside the EU or the UK can access data originating in the EU or in the UK. This is largely for troubleshooting, fixing systems errors/ defects, and support purposes. Those who require access to customer data sets must go through a formal approval process authorized by Phenom leadership teams. Robust controls have also been implemented to prevent and restrict downloading or transferring of any data. Employees located outside of the EU or UK are provided with read-only access to EU or UK customer data.

Robust encryption measures that are industry-standard — both when the data is in transit TLS 1.2 and at rest AES 256.

Updating customer contracts to include the new Standard Contractual Clauses issued by the European Commission.

TAKE ACTION
GDPR Compliance Checklist

In order to meet GDPR compliance, there are a few steps that you will need to take:

Assign an email inbox that Phenom can leverage for any GDPR request notifications from candidates visiting your career site(s).

Assign an administrator to monitor GDPR requests. This administrator will be provisioned with a Phenom account to take GDPR actions outlined above.

Review Phenom's Privacy Policy that is recommended to be included in your existing privacy policy (provided by Phenom).

For additional details or questions, please contact your Customer Success Manager.

phenom

Phenom is a global HR technology company that delivers its AI-powered Talent Experience Management (TXM) platform to enterprises, enabling them to help candidates and employees find the right job, recruiters identify and engage the right talent, and management optimize HR strategy, process, and spend. The Phenom TXM platform is built on artificial intelligence (AI), driving personalization, automation, and accuracy for candidates, recruiters, employees, and hiring managers. It eliminates multiple-point solutions, delivering top talent and driving ROI.

phenom.com