5 Common GDPR and Candidate Privacy Questions Answered

LEVER

Introduction

The general data protection regulation (GDPR) was put into place in 2016 and became enforceable in 2018. Since then, any organization that collects personal data from someone in the European Union (EU) is subject to rules around how that data is collected, stored, and processed.

As the recruiting and hiring industry increasingly comes to use online data to identify and reach out to prospective candidates, laws like GDPR have had more influence on hiring and recruiting practices. Candidates have also become more aware of the issue of privacy and personal data, making GDPR compliance a sound priority both for the legal ramifications and the cause of building trust with candidates.

For recruiters and hiring managers navigating this murky world of candidate data, however, there's a lot that's left unclear. And that's intentional – the GDPR does not offer a one-size-fits-all interpretation of what to do or why, so it's important organizations consult with general counsel to set up their unique approach to GDPR based on their size, location, and level of risk tolerance.

While you don't need to be a data protection specialist to recruit and hire today, it does help to have a basic understanding of how GDPR affects your work. In this eBook, we'll explore the five important questions everyone must ask about their GDPR policy — and how the answers should affect the way your organization collects, processes, and stores candidate data.

IN THIS EBOOK

Translating the GDPR for Recruiters

When discussing GDPR and how it relates to recruiting, a little translation is necessary. Here's how the data-focused terminology of the GDPR applies to recruiters, candidates, and technology:

- **Data Subjects** refer to the candidates being recruited. The GDPR exists to protect candidates and regulate how companies use or collect their personal data.
- **Data Controllers** refer to the companies or the recruiters that are collecting the data subjects' personal information.
- **Data Processors** refer to the systems and platforms that are used to capture and process personal information, such as an applicant tracking system (ATS) or talent management platform.

The GDPR states that data controllers (the employer) must clearly disclose any data collection and declare the lawful basis and purpose for data processing (collecting candidates' personal information). They must state how long data is being retained and if it is being shared with any third parties or outside of the EU.

Data subjects (candidates) have the right to request a portable copy of the data collected by a controller in a common format, and have the right to have their data erased under certain circumstances.

01 What is GDPR?

GDPR is a regulation within the EU that gives individuals control over their personal data. It defines personal data as any information related to a person, such as their name, photos, email addresses, bank details, updates on social networking websites, location details, medical information, and computer IP address. GDPR does not make a distinction between an individual's personal data or professional data.

When it comes to recruiting and hiring, GDPR requires that companies must clearly disclose any data processing and declare the lawful basis and purpose for the processing. They must also state how long data is being retained, and if it is being shared with any third parties or outside of the EU.

Because of its stance on privacy protection, the GDPR has become a model for many national laws outside of the EU, including The California Consumer Privacy Act (CCPA) and its likely successor California Public Records Act (CRPA), as well as the General Data Protection Law (LGPD) in Brazil.

02 How does the GDPR affect my organization?

If your company hires candidates who reside within the EU, regardless of whether the processing takes place in the EU or not, GDPR applies to you, and you'll need to be able to demonstrate compliance.

Article 6 of the GDPR outlines the six conditions, of which one must be met, in order for there to be a legal reason for processing the data:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

The two most common bases for retaining the information recruiters and hiring managers meet is:

1. Receiving consent from a candidate at the start of the application process
2. Demonstrating that your company has a legitimate interest for a business purpose that is not outweighed by rights and freedom of the individual

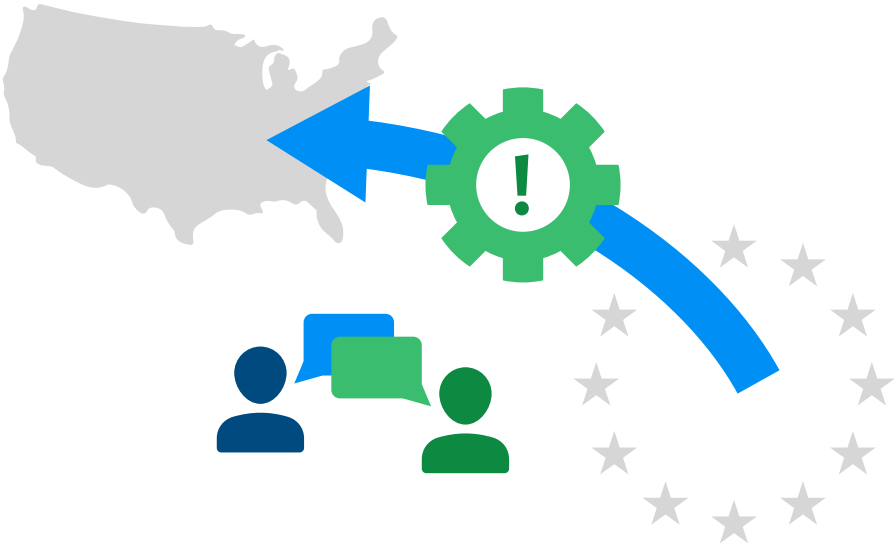
The critical factor for proving consent is that all personal data being collected and stored needs to have an accessible audit trail that outlines precisely when and how the consent was provided. A good talent management platform or ATS should have a way to easily collect consent, whether it is as simple as a check box for candidates to mark or a more structured consent field.

If an organization cannot prove that they meet one of the six conditions and is found to not be in compliance, they face strict penalties, up to a maximum of 4% annual global revenue or €20 million, whichever is higher.

03 How does this fit into global policies around recruiting and hiring?

When companies transfer recruiting and hiring information outside of the EU, such as in the event a candidate applies for a job on a talent management platform based in the United States, the GDPR requires that a lawful transfer mechanism be in place.

Different factors affect this lawful transfer mechanism, which is why it's so important to discuss this topic with counsel and work with a talent management partner who understands these nuances.



04 How seriously should we take GDPR?

While the GDPR establishes data privacy principles, it does not detail exactly how these principles should be achieved. Decisions regarding how companies achieve compliance are unique to each organization and subject to different factors, like the size, location, and risk tolerance of your organization. The best way to make a plan is to work with legal experts that understand how your business operates, and what level of risk tolerance your organization is comfortable with.

At Lever, we facilitate the varying ranges of compliance strategy or risk tolerance among our customers by offering customizable functionality when it comes to GDPR compliance. In that way, we can accommodate various levels of risk tolerance and provide each customer exactly what they need.

05 How does talent management software help with GDPR compliance?

The most important thing a talent management platform or ATS can do to assist recruiters and hiring managers with GDPR is to provide options. Different organizations will have different approaches to GDPR, so the ability to customize how you collect candidate data is incredibly powerful.

Here are a few of the most important ways your choice in technology can support GDPR compliance — automating these functions to prevent GDPR from being a burden on operations within your organization:

- Offers a clear way for candidates to give consent in a legal manner, easily remove consent, and request access to their data
- Provides a way to confirm data has been removed from all platforms when a candidate requests it
- Provides a method to share a copy of all candidate data when requested by candidate
- Ensures the ability to report on a breach in data within 72 hours of determining that it is likely to result in a risk for the rights and freedoms of individuals

Conclusion

The consequences of non-compliance with GDPR don't stop at fines and legal action. GDPR also represents a new take on what candidates expect from companies when it comes to their personal, private data — so it's up to you to make sure your approach offers an accurate impression of how much you respect candidate privacy and consent.

To learn more about Lever's commitment to privacy and secure talent relationship management platform, reach out to a representative to learn more.

LEVER

About Lever

Lever's mission is to help the world hire with more predictability. Lever is transforming the way companies hire through an approach that allows talent leaders to attract candidates like a marketing leader, forecast like a sales leader, and have the insights of a finance leader.

For more information, visit lever.co  LeverApp  Lever  @lever


LEVER