Everything Recruiters Need To Know About GDPR

ZOHO Recruit

zoho.com/recruit

Increasing concern for data privacy has inspired many government and regulatory agencies take immediate action, leading to the creation of new legislation that aims to protect personal data.

The EU General Data Protection Regulation (GDPR) was designed to standardize laws across Europe, to protect and empower EU residents, and to reshape the way organizations in the region approach data privacy.

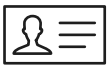
The GDPR covers not just EU residents and businesses, but anyone who handles data from those in the region.

As the legal initiation date for GDPR approaches, we've compiled important compliance information to make sure your business is ready for these new data privacy regulations.

INDEX

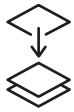
KEY TERMS

Before we describe how GDPR will affect your recruiting efforts, it's important to have a clear understanding of the language used in the law. Knowing key terms will ensure that everyone involved in the recruiting process complies with this new set of regulations.



Personal Data is any information that can be used to identify a data subject. Many types of information fall under this category, but for recruiters, the most common types of personal data are the candidate's phone number, date of birth, and email address.

Data Subjects are your candidates or anyone who provides personal, identifying information to a recruiter, hiring manager, or business professional.

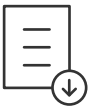


Data Controllers decide what to do with personal data and how to process it. Recruiters are in control of multiple data subjects' information.

Data Processors handle data on behalf of a data controller. This could be your recruitment software (like Zoho Recruit).

Data Processing refers to any action performed on personal data such as storing, collecting, recording, organizing, processing, or erasing any candidate or client record.

DATA SUBJECTS HAVE THE FOLLOWING RIGHTS UNDER GDPR:



1. The Right to Access

Upon request, you will need to provide candidates with a copy of their data in electronic format, free of cost.

2. The Right of Rectification

When a candidate tells you that their information is incomplete or incorrect, you must verify and update their information in your candidate database immediately.

3. The Right to Be Forgotten

You will need to delete candidate data from your database if:

a. You obtained the data without the candidate's consent.

b. The candidate withdrew consent to process their data.

c. The candidate's data is no longer relevant to your recruitment processes.

d. The candidate objects to the processing of their data.

4. Data Portability

Candidates have the right to receive their personal data. You must export their personal data into a machine readable format (such as XML, JSON, CSV, TSV, XLS, etc) and hand it over to the candidate.

5. The Right to Object and The Right to Restriction of Processing

These two rights are somewhat related and you should cease processing a candidate's data if the data is found to be inaccurate, or if you obtained the information without consent. You must also stop processing candidate data upon request, regardless of reason.

FOR RECRUITING AGENCIES AND EMPLOYERS

Under GDPR, recruiters and employers have new legal responsibilities regarding how they handle candidate information. Consequently, it's important to make sure your privacy notice is easily accessible to anyone applying for a job. This document should detail how you collect candidate data and what you do keep the data secure.

For the purposes of recruiting, there are two important stages during which a candidate will share their personal data: initial application and processing. It is the recruiter's responsibility to be fair and transparent while handling any personal data during these two stages.

When a candidate applies for a position:

- Provide contact information of your company or its representatives.
- Explain why you're processing the candidate's data, and assure them that you're using this information for recruitment reasons only.

Note: Staffing agencies should disclose their clients' information to candidates when requested under specific circumstances.

After receiving applications, provide candidates with additional information:

- Explain why you're storing the candidates' data.
- Inform the candidate how long you'll store their data. The GDPR states that personal data may be retained for only as long as is necessary therefore, ensure your candidates know how long you will retain their data in your systems and the purpose for the same (this can be covered in your privacy notice too).
- Provide your contact information in case the candidate wants to access, correct, or erase their personal data (data controller's contact information).
- Explain how candidates can withdraw their consent or restrict the processing of their data.
- Provide contact information in case the candidate wants to file a complaint regarding the processing of their data (Data Protection Officer's contact information).

Note: If you want to use the candidate's data for any purpose other than recruitment, you must obtain their explicit consent before processing their data.

If you source candidates via the web, or obtain their details through other methods, you should provide the following information:

1. The source from where the candidate's data was obtained.

2. The name and the contact information of your company or its representatives.

3. The purpose of processing the candidate's data. You will have to make sure to use the candidate's data for recruitment reasons only.

4. The length of time you will store the candidate's data. The GDPR makes it clear that personal data may be retained for only as long as it is necessary. If it is not possible to give an exact time period, you will need to provide an approximate timeline.

5. How candidates can contact you in case they want to access, correct, or erase their personal data.

6. How candidates can withdraw their consent or restrict the processing of their data.

7. Contact information in case candidates want to file a complaint regarding the processing of their data.

8. In case you are a staffing agency (hiring for your clients), you may have to disclose your clients' information to the candidate.

Only after the candidates give their consent, can their information be processed on your end. During that time, candidates can invoke their rights within the GDPR and you must act accordingly immediately.

GDPR also offers a set of guidelines for when a processor handles candidate information on your behalf.

Compliance for Applicant Tracking Systems (ATS)

According to GDPR, Zoho Recruit is a data processor that handles a candidate's data on behalf of a recruiter. In order to stay compliant, such systems must be governed by a data protection agreement (DPA) that's set up by the data controller. The contract will require the ATS to:

1. Process the candidate's data as specified in the contract set up by the controller.

2. Implement necessary measures to safeguard data, such as:
    a. Choose an ATS provider who prioritizes data security.
    a. Test, evaluate, and maintain data security
    b. Encrypt of candidate data
    c. Restore candidates' data in case of incident

3. Demonstrate the ATS' commitment to the Data Controller in supporting them in their compliance journey like.
    1. Providing options to the Data Controllers for catering to the data subjects when they exercise their rights.
    2. Notify of any data breach at their side on time so that the Data Controller can carry forward their obligations.

If an ATS integrates with external applications, it's mandatory that those external apps also be GDPR compliant.

GDPR TIPS

1. Discuss your Terms and Conditions with your legal team.

People with expertise in GDPR and regulatory issues can give you a checklist of how to stay in compliance.

2. Get a second nod from your candidates. Avoid issues down the road by double checking that candidates consent to storing their resumes in your database for future hiring possibilities.

3. Make sure your ATS is GDPR compliant. Although you're the data controller, most of the work is done by a processor, such as an ATS.

4. Keep your candidates in the know. Offer all pertinent data-related information the first time you reach out to a candidate, including details about the client(s) with whom you might share candidate data.

5. Review current security and privacy processes. Revise your contracts with third parties vendors and customers to meet GDPR requirements.

6. Streamline your candidate database. Failure to comply with GDPR can result in fines of up to €20 million.

7. Fast is fine but accuracy is everything. Always maintain accurate and latest data in your systems.

8. Avoid holding off. Don't retain data for long just because you think you might require it later.

9. Delete data once the purpose is solved. You might have collected candidates' blood groups during their hiring process. Once the process is done and you no longer need the supplementary info, delete it. The more data you hold, the more liable you are.

To summarize, collect candidate data only for recruitment purposes, and remember to explain not only the extent of data processing but also how long their data will be stored in your system. Ask for the candidate's consent at all times before processing the data. If the data is no longer required, remove the candidate's information from your system.

HAPPY RECRUITING!

ABOUT ZOHO RECRUIT

Zoho Recruit is all about building great teams and hiring the best talent without breaking a sweat. Our all-in-one applicant tracking system helps teams of all sizes source, track, and hire candidates.

Zoho Recruit has been an unparalleled champion in many software categories for two years and running.

Visit us at zoho.com/recruit