Jobvite

Is Consent Required?

GDPR & RECRUITING: CONSENT VS LEGITIMATE INTERESTS

By:
Kimberley Smathers
Security & Privacy Officer
Jobvite

GDPR & Recruiting

Is Consent Required?

One of the most confusing terms related to the GDPR and recruiting is something called 'Legitimate Interests.' Some recruiters and marketers are attempting to use it as a 'Get out of jail free card,' when considering whether consent is required in recruiting and marketing activities.

The "legitimate interest" provision in the GDPR will not save recruiters and recruiting software from the challenge of obtaining consent for personally identifiable data. Even so, some in the recruiting space believe that they can continue to use personal data without consent because of an apparent carve-out related to "legitimate interest" contained in the GDPR.

The short answer to this belief is…No, Not True.

Unfortunately, the reason that this is such a confusing issue is that there are multiple parts of the law (Articles, Recitals, and Definitions) that have to be applied to arrive at an answer as to when Consent is required or Legitimate Interests is adequate with regard to processing personal data.

First, let's identify a few key terms and definitions:

Reference	Type of Information	Meaning
Article 6	Article of the GDPR laws	Covers what is 'lawful' processing under the law
Recital 47	Recitals are interpretations of specific parts of the Article of the GDPR	Specifically relates to the subject of 'Overriding legitimate business interest' as referenced in Article 6
Consent	Definitions and Terminology of the GDPR	Explicit definition of what comprises lawful processing of the personal data of a data subject under the GDPR
Legitimate Interest	Definitions and Terminology of the GDPR	Explicit definition of what legitimate business interest is
Legitimate Interest Assessment	Template	Used to establish whether legitimate interest is valid
Relevant and Appropriate Relationship	Description	Required to establish a legitimate interest

Now, Let's examine what is meant by consent under the law;

> "Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

And, next, let's add Article 6, Lawfulness of Processing:

Article 6 sets out the conditions for lawful processing of personal data and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing and in relation to a specific purpose;

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) 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;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) 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;
f) **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.

It's easy to identify which of these will apply in the recruiting space; bases A and F; A is clearly using consent to lawfully process the data, and F indicates that, if valid 'legitimate interests' are present and not overridden by data subject rights, then data subject consent is not required – only a valid 'legitimate interest.'

So, clearly, when performing recruiting activities i.e.; seeking candidates for the purpose of employment, an organization is requesting personal data that will be processed and stored, and so, must either obtain consent or communicate a legitimate interest.

Easy, right? Recruiting applicants seems like a 'legitimate interest,' so, why bother with the challenge of obtaining and recording consent?

There are some in the recruiting space currently communicating just that, consent isn't necessary because of Recital 47, 'Overriding Legitimate Interest.' The problem with this is that legitimate interests is widely misunderstood and requires a lot more than simply saying it exists for your organization and, in the case of recruiting software providers (like Jobvite), saying that customers (Controllers) don't require it.

Why?

Let's take a look at Recital 47

Under Recital 47 the legitimate business interests of a controller (recruiting organization),

*"including those of a controller to which the personal data may be disclosed, or of a third party, **may** provide a legal basis for processing,* ***provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller****."*

What? It certainly sounds like you might not need to get consent.....let's read on before we celebrate

Let' s break down Recital 47 a bit before we move one – it will be important in order for us to arrive at a conclusion.

Take note of the use of the word **'may'** in the statement – it means that an assessment must be undertaken to analyze and prove whether the legal basis exists. Effectively, it is possible that there is a legal basis for the processing – but must be assessed and proven valid.

What is a legitimate interest?

A legitimate interest is "***a clearly articulated benefit to a single company, or to society as a whole, that can be derived from processing personal data in a lawful way***." However, the Article 29 Working Party of data protection authorities of EU countries has already made it clear that "***merely having a legitimate interest does not entitle one to use personal data***."

What is the Relationship with Controller?

Where there is a relevant and appropriate relationship between the individual and the Controller is in situations where the individual (data subject) is a client or in the service of the organization. However, this does not mean that there will always be a Legitimate Interest in processing an individual's data. ***Legitimate Interests is more likely to apply when there is a direct 'appropriate' relationship with a data subject*** because the processing is less likely to be unexpected or unwanted. Recital 47 indicates that it is "**more difficult to use Legitimate Interests when there is no pre-existing relevant relationship**." In the recruiting of job seekers no pre-existing relationship exists.

Well, that's confusing, isn't it?

Let's continue to break it down:

The existence of a legitimate interest requires a formal and careful assessment to prove that the interest exists and is valid.

An essential part of the concept of Legitimate Interests is the balance between the interests of the Controller and the rights and freedoms of the individual: '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.'

Legitimate Interests Assessment

In order to establish Legitimate Interests an organization must perform a formal assessment and document the process and results making them available to **data subjects, data authorities,**

and the courts in order that they can examine the assessment. The assessment must include the following:

Identify a Legitimate Interest

The first stage is to identify a legitimate interest – what is the purpose for processing the Personal Data and why is it important to you as a Controller? A legitimate interest may be elective or business critical; however, even if the Controller's interest in processing Personal Data for a specific purpose is obvious and legitimate, based on the objectives of the Controller, **it must be a clearly articulated and communicated to the individual.** Which assumes an existing relationship – which, in recruiting, does not exist.

Carry out a Necessity Test

Controllers should consider whether the processing of Personal Data is "necessary" for the pursuit of its commercial or business objectives. The adjective "necessary" is not synonymous with "indispensable" but neither is it as wide as "ordinary", "useful", "reasonable" or "desirable". It may be easiest to simply ask, "**Is there another way of achieving the identified interest?"** If there isn't, then clearly the processing is necessary; or If there is another way but it would require disproportionate effort, then you may determine that the processing is still necessary; or **If there are multiple ways of achieving the objective, then a Data Protection Impact Assessment (DPIA) should be used to identify the least intrusive processing activity**; or **If the processing is not necessary then legitimate interests cannot be relied on as a lawful basis for that processing activity.**

The Balancing Test

Article 6 (f) of the GDPR includes the following important caveat: "except where such interests are **overridden by the interests or fundamental rights and freedoms of the data subject**". In other words, a business that intends to use personal data **must balance its legitimate interest not only against the rights of the data subject, which is a significant test in itself, but also the data subject's interests,** irrespective of whether these interests are legitimate or not. Any company that hopes to use legitimate interest also bears the onus for demonstrating that its interest is favored in such a balancing test.

This is not a figurative exercise. The Article 29 Working Party cautions that the balancing test should be **documented in such a way that data subjects, data authorities, and the courts can examine the assessment**. It should encompass a broad range of factors including "any possible (potential or actual) consequences of data processing". This would include, for example, "broader emotional impacts" and the "chilling effect on … freedom of research or free speech, that may result from continuous monitoring/tracking".

The test also must consider the manner in which personal data are processed. For example,

> "whether large amounts of personal data are processed or combined with other data (e.g. in the case of profiling…). Seemingly innocuous data, when processed on a large scale and combined with other data may lead to inferences about more sensitive data".

Europe's data protection authorities take a dim view of such large scale processing:

> "Such analysis may lead to uncanny, unexpected, and sometimes also inaccurate predictions, for example, concerning the behavior or personality of the individuals concerned. Depending on the nature and impact of these predictions, this may be highly intrusive to the individual's privacy".

A further factor in the balancing test is mentioned in Recital 47 of the GDPR: "…taking into consideration the reasonable expectation of data subjects based on their relationship to the controller". A business involved in recruiting must ask the following question: Is it reasonable to assume that a regular person who wishes to submit interest in a job opening expects that their behavior is being tracked and measured, their data shared with other companies or recruiters, and that the results of these operations may be between different organizations, and retained for further consolidation over considerable periods of time?

Why does this matter to you?

Your organization is the Data Controller in all of this – **your organization is responsible** for obtaining consent or proving legitimate interest - **not your recruiting solution**. After reviewing all of this information it is pretty apparent that;

Consent – and nothing short of it – is the necessary legal basis for processing personal data for recruiting.

Any recruiting solution that does not provide you with the tools to comply with GDPR – and collect consent from your applicants – exposes your organization to risks and liabilities that include significant fines - Up to €20 million, or 4% of an organizations worldwide annual revenue.

If you are reviewing a recruiting solution with no tools for consent and compliance consider that your organization will need to perform the assessment described above in order to legally process personal data without obtaining consent.

Ultimately, it seems like a pretty easy choice when deciding on a recruiting solution – choose one that provides the tools to ensure your compliance under the law and reduces your exposure to fines and liabilities.