



SmartPaper

Is Your Recruiting Data GDPR Compliant?

EU DATA PRIVACY COMPLIANCE

by Jennifer Goode



Introduction

We live in unprecedented times. The rapid pace and spread of digital technologies has fundamentally and globally transformed the way we connect, the way we learn, the way we do business, and, incredibly personal to our mission, the way we engage and hire talent. A byproduct of this expansive interconnectivity is the tremendous explosion of data now produced on a continuous basis. To put data levels into perspective, and according to a recent Cisco forecast report, it would take more than 5 million years for an individual to watch the amount of video (as one example) that crosses global IP networks each month in the year 2020.* 5 million years! Attempting to comprehend this amount of data is unfathomable, and, yet, poses real challenges to organizations operating around the globe, requiring them to think differently about how to process, transfer, store, and protect this enormous amount of data.

Elsewhere, this level of data presents serious challenges in the form of privacy concerns, specific to the dissemination and accessibility of personal data. A consequence, for better or worse, of living in this digital age is the sheer volume of personal data necessary for online transactions, whether applying for a job, engaging in social networking, or purchasing professional services, among other interactions. Data privacy concerns have prompted a number of government and regulatory agencies around the globe to take action via creation of new legislation aimed at the security and protection of personal data. Consequently, this legislation imposes new obligations on those businesses who process and collect personal data - **and this includes the data you collect from applicants as part of your recruiting process.**

Specifically, the General Data Protection Regulation is one such piece of legislation that could have a major impact on the recruiting data collected by our customers during their recruiting process. So, to help shed some light on this new legislation, this discussion will address the following questions:



What is the general data protection regulation (GDPR) ?



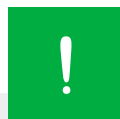
Who does it impact?



What data does it cover?



How is compliance demonstrated?



What are the specific obligations for data processing?



Please look for sections signified with a colored bulb to denote how SmartRecruiters customers benefit dealing with their GDPR compliance



The General Data Protection Regulation

The European Commission, a regulatory institution of the European Union (EU) that oversees, regulates, and manages the daily business of the EU, recognized serious gaps in its Data Protection Directive (DPR), a policy that was intended to provide guidelines for the protection of personal data, but fell short in offering a unified approach for data privacy in light of new technological advancements and increased volume of personal data. These gaps created a number of problems for companies doing business in the EU. For example, EU Member States were left to their own for creating data protection policies making compliance difficult across different jurisdictions, while individuals were left without a real avenue of enforcement for protecting their personal data. As a result, the ability to conduct business across Member States - for organizations both foreign and domestic - became increasingly burdensome. In an effort to strengthen rights of EU citizens and streamline the various data privacy policies of Member States,

while also modernizing and strengthen data protection laws across the EU, the European Commission enacted new legislation on May 4, 2016, known as the General Data Protection Regulation (GDPR). The GDPR requires organizations to be legally compliant in their data processing activities, or face severe financial penalties to the tune of \$20-million or 4% of worldwide revenue (whichever the greatest), for non-compliance. Ouch. Thus, it's no surprise this dramatic increase in monetary penalties for non-compliance, a stark departure from the mere guidelines of the DPR, caused ripples of concern across organizations that both conduct business in the EU, or, alternatively, offer services or goods to EU residents. The sweeping impact and the increased territorial scope of the GDPR has earned itself recognition as one of the most protective privacy systems in the world, with real consequences for businesses that fail to comply.



SmartRecruiters is your Partner for Data Privacy

At SmartRecruiters, we recognize this new legislation directly impacts many of our valued customers, both in the U.S. and abroad, while also presenting real apprehension (and in some cases dread) given the severe monetary penalties that will be imposed. Believe us when we say, “We get it!” - and as your Talent Acquisition Data Processor - we also share in these new compliance responsibilities. So, when it comes to navigating data privacy concerns, we’re here for you, and we’re in this together!



The GDPR requires organizations be compliant **today**. That said, penalties are suspended until this transition is completed, which is less than a year from the time of this paper’s publication, May 31, 2017, according to the official GDPR website countdown, which you may track at - www.eu-gdpr.org/eugdpr.org.html. The European Commission recognizes the significant time and effort it takes for ensuring transparency, compliance, and uniformity with these new obligations. As, arguably, the most lobbied piece of legislation in EU history (it took more than four years to negotiate!), this process does not happen overnight. As such, the GDPR won’t become legally enforceable until May, 25, 2018.

So, as your partner in data privacy, SmartRecruiters offers this overview, which serves to highlight the GDPR’s key provisions and obligations our customers ought to consider to ensure

the recruiting data collection is performed in a manner that is GDPR-compliant.

Keep in mind, because we are not lawyers, we are not at liberty to give you or your organization legal advice.

In light of the significant monetary penalties imposed for non-compliance with the GDPR, we strongly recommend your organization consult with legal professionals who specialize in EU data privacy protection so you (and your revenues) are sufficiently protected.

The information we provide in this paper is intended to inform our customers of the potential impact GDPR may have on their recruiting data and to highlight where the SmartRecruiters platform can help facilitate meeting your compliance objectives. That said, this discussion is in no way a substitute for sound legal advice, which is always recommended.



Who is Impacted by the GDPR?

The GDPR expands the scope of data privacy regulations to almost every company in every industry that conducts business in the EU, regardless of its location.

All Companies that Conduct Business in the EU — Unlike its predecessor the Data Protection Regulation (DPR), the newly-enacted GDPR goes much further in its governance of data privacy with an expanded scope of jurisdiction that includes all businesses based in the EU, and/or conducting business in the EU. This means whether you are a company located and operating in the EU, or, alternatively, outside the EU but provide goods and services to EU citizens - you must comply with the GDPR.

[Where Can I Learn More](#) → *GDPR, Chapter 1: General Provisions, Article 3*

Data Subjects, Controllers and Processors — The GDPR identifies and governs three classifications that fall within business transactions, that either have personal data rights or, alternatively, personal data obligations under this law. These groups are classified as Data Subjects, Data Controllers, or Data Processors.

Data Subjects — At its very core, the GDPR is centered on strengthening and protecting the rights of individuals - called DataSubjects in the GDPR - which are essentially “natural persons,” or rather citizens residing in the EU who supply their personal data for some sort of business transaction.



In SmartRecruiters, Data Subjects are your Applicants and Candidates, who express interest, supply a resume, complete an application, etc., when pursuing employment opportunities with your organization.

Data Controllers — According to GDPR language, Data Controllers are defined as the entity that determines what type of personal data is required, in addition to the purpose for how and why personal data is used.



As a SmartRecruiters customer, YOU are the Data Controller because you determine the purpose, the reason, and type of information collected from your applicants and candidates. Essentially, this information is the data you need for evaluating one’s skills and experience necessary for making a hiring decision.


Data Processors — The GDPR identifies Data Processors as those entities that process data on behalf of the data controller, and as directed by the data controller. Remember, the definition of “data processing” is quite broad and includes actions such as collecting, recording, organizing, storing, retrieving, etc.



Here, SmartRecruiters is your Data Processor, as our platform serves to process the data you control and instruct us to collect as part of your hiring process.

[Where Can I Learn More](#) → *GDPR, Chapter 1: General Provisions, Article 3*

Accordingly, SmartRecruiters and its Customers are both subject to the GDPR. That said, our obligations under the GDPR will differ based on our role as Data Processor and Data Controller, respectively. We’ll cover these specific obligations a bit later.



What is Covered by the GDPR?

While the GDPR is extensive in its reach of who is impacted, its focus is more narrow in terms of what is impacted.

Data Processing — The GDPR only applies to the act of data processing, albeit the actual definition of what activity constitutes data processing is quite broad. For example, companies performing any sort of activity that in any way or shape involves or affects the personal data of another, such activity qualifies as data processing - and may only continue if performed in a manner that is compliant with the provisions of the GDPR.

Specifically, the GDPR defines data processing “as any operation performed on personal data,” whether or not by automated means, and includes (but is not limited to) the collection, use, recording, organization, storage, etc., of personal data. Thus, any time a business or organization does virtually any activity - electronic or manual - that touches or involves personal data, the GDPR applies.


 Relevant to your recruiting processes, the activity of requesting information from an applicant or candidate when he or she applies to a job posting, and/or you require as part of your job application process, whether manually collected or, alternatively, leveraging a tool like SmartRecruiters, qualifies as data processing activity under the GDPR.

 **Where Can I Learn More** → *GDPR, Chapter 1: General Provisions, Article 2 & GDPR, Chapter 1: General Provisions, Article 4*

Personal Data — While the GDPR applies to data processing activities, its provisions are only enforceable where the data processing activities involve personal data. Personal data is also broadly defined in the GDPR as “any information related to a natural person or ‘Data Subject’, that can be used to directly or indirectly to identify the person.”

To provide some perspective, most U.S. companies are familiar with the term P.I.I., which stands for Personally Identifiable Information, and is generally defined to cover very specific and very personal pieces of information like ‘Date of Birth’ or ‘Social Security Number,’ etc., or rather highly-sensitive personal information that warrants a particular duty of care by a Data Controller.

Different, the European Commission simply speaks in terms of “personal information,” which encompasses a great deal more than the U.S. definition of PII. In other words, you would be hard-pressed to find an example of information that does not qualify as “personal data” under the GDPR.

 As this relates to your hiring process, most, if not all, of the information you collect or request from an EU applicant or candidate in your hiring process, including whatever personal information you collect leveraging the SmartRecruiters platform, falls within this broadly-defined concept of personal data. For these reasons, many of our customers may want to restrict access to who on their hiring team has access some of this data. To accommodate this request, SmartRecruiters offers role-based security configurability so your Admin users may control permissions and access of your users within the platform.

Understanding what activity is specifically covered by the GDPR - as discussed above - only serves to reinforce the applicability of the GDPR to your EU recruiting activities where personal information is involved.

 **Where Can I Learn More** → *GDPR, Chapter 1: General Provisions, Article 2 & GDPR, Chapter 1: General Provisions, Article 4*



What are the Principles for Compliance?

Let's recap. Whether you are located in the EU or, alternatively, located elsewhere but conducting business in the EU, any of your data processing activities involving personal data of EU citizens, **must comply with GDPR principles** to be lawfully permitted.



For SmartRecruiters customers, this applies to the recruiting and hiring activities you perform while leveraging our platform that involves collection of your candidates' personal information.

So, the next logical question is - what are the principles you need to follow to be compliant with the GDPR?

Specific to the GDPR's protections for Data Subjects, there are several principles that are key for processing personal data. This discussion highlights five (5) of these principles that must be met relevant for processing personal data, which provides an accountability framework for Data Controllers:

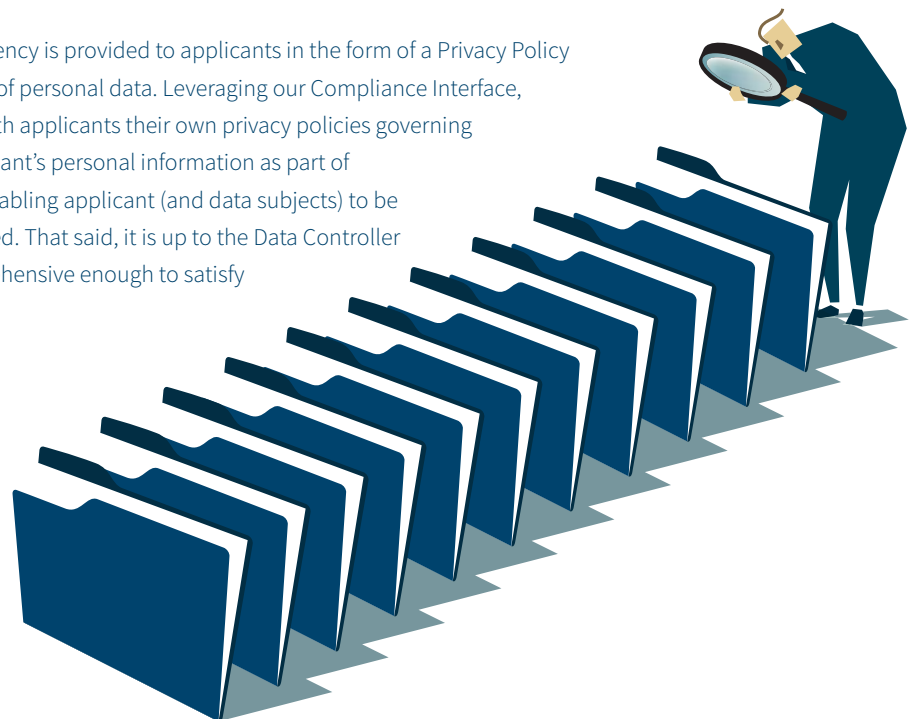
PRINCIPLE 1 - "FAIR AND LAWFUL WITH TRANSPARENCY" — Data Processing activities involving personal information must be performed in a fair and lawful way, as well as in a manner that provides transparency to the data subject. So, namely, Principle 1 involves two elements that must be satisfied:

Transparency - Transparency is accomplished by informing the data subject what data of his or hers is or will be processed, and how that data will be used. Hence, there must be "transparency" around processing activities. So, personal data cannot be processed unless the data subject knows about it.

Hence, it is important for you - the data controller - to think about how you will provide such notice to your job applicants, especially when using a data collection tool or recruitment software as the means for facilitating your hiring process. Ask yourself, when a candidate applies - have we informed them about what information we collect and how it will be used?



In SmartRecruiters, for example, transparency is provided to applicants in the form of a Privacy Policy that covers acceptable access to and use of personal data. Leveraging our Compliance Interface, SmartRecruiters Customers may share with applicants their own privacy policies governing the collection and processing of an applicant's personal information as part of the job application and hiring process, enabling applicant (and data subjects) to be informed about how their data will be used. That said, it is up to the Data Controller for ensuring their Privacy Policy is comprehensive enough to satisfy GDPR's transparency element.




Fair and Lawful - To show that Data Processing activities are performed in a fair and lawful manner requires Data Controllers to show at least one of the following conditions exist:

- Data Subject Consents to Data Processing
- Data Processing Protects Vital Interests of Data Subject
- Data Processing is Necessary for Contract Performance
- Data Processing in the Public Interest
- Data Processing is Part of a Legal Obligation
- Data Processing Necessary for Controller's Legitimate Interest

Obviously, not all of these conditions are relevant to your hiring process. The most logical conditions to demonstrate “fair and lawful” data processing for processing a job applicant would likely be consent - i.e. the applicant consented to the process - and/or legitimate interest - i.e. this data is relied upon by our business to hire qualified employees and meet growth objectives. Whichever condition is most relevant to your data processing activities - remember, you, the data controller must show one of these conditions exists.

Note, if relying on consent, the GDPR requires it to be explicit — meaning the applicant (data subject) must have explicitly consented to his or her data being processed. It is not enough to say the simple act of applying qualifies as implied consent. Consent must take on the form of an express action whereas a candidate actually checks a box or overtly selects an option to move forward/continue and such action is recorded. If your organization relies on a candidate's consent for demonstrating lawfulness - we suggest you familiarize yourself with the relevant GDPR provisions and accompanying recitals that speak to consent as it has become more tricky to provide under GDPR (see reference in blue below).

 SmartRecruiters Global Compliance Center - part of our Global Subscription package - provides functionality for customers to display their relevant privacy policies, should they opt to provide these to their applicants. For more information, on our Global Compliance Center, please follow up with our sales team or your dedicated Customer Success Manager for more information.

 [Where Can I Learn More](#) → *GDPR, Chapter 2: Lawfulness, Article 6 & GDPR Recitals - 40 through 47*

PRINCIPLE 2 - “EXPLICITLY SPECIFIED” — Personal Data may only be processed for a specific and limited purpose. This means personal data processed for one purpose, cannot then be processed for another. In other words, the purpose of the data processing must be explicitly specified.





Use Case

Let's provide a recruiting example to highlight this rule. YOU - the Data Controller - request the email address (processing) of Data Subject "Applicant A" and inform "Applicant A" you will only use the email provided for communicating information with him or her during the hiring process of Position 1. "Applicant A" consents to this use and provides you the email address (personal information).

The hiring process of Position 1 concludes because the vacancy was filled with a different applicant, and you inform "Applicant A" of this news, thereby ending Hiring Process 1. However, in your opinion "Applicant A" was a really great candidate, and likely a better fit elsewhere. So, you decide to keep "Applicant A's" email for sharing information about future opportunities. Would this be permitted?

The answer is a very likely, No, pursuant to the "specific and limited" rule. Here, "Applicant A" was told the email address is only for hiring process communications pertaining to Position 1. At no time was it communicated that the email address would be used for future opportunities. Hence, the personal data (email address) provided to you - the Data Controller - was explicitly stated for communications purposes related to Position 1.

Should the specific purpose be communicated differently, here, say "used for communications about this position and for any future openings," then any communications about future positions would then be permissible in this example because the specific and explicit use included Position 1 and future opportunities.



So, as you prepare for compliance with the GDPR, it is critical to think about how you plan to use candidate data in SmartRecruiters when communicating its explicit purpose for data processing with your candidates, such that you do not fall in violation of this rule.

Remember, personal data explicitly specified for one purpose may not be used for another - so be clear and comprehensive in your notice to data subjects.

PRINCIPLE 3 - "ONLY WHAT IS NECESSARY" — Data Controllers are further limited in their data processing activities to the extent they may only use that data which is absolutely necessary for achieving their purpose. In other words, Controllers must minimize the amount of personal data they process, limiting processing activities to only critical personal data.

This requires Data Controllers to be thoughtful about their data processing activities - discerning between personal data that is nice to have vs. personal data that is necessary. So, what is the litmus test for determining "only what is necessary"? The GDPR is silent, here, and places the burden on the Data Controller to make that determination, as it depends on the circumstances of the data processing activity.




Relevant to our platform, SmartRecruiters' productized application and job advertisement process serve to standardize and limit the amount of personal data collected from applicants, thereby enabling customers to more easily identify what information is critical and necessary for efficient and effective recruiting that produces the best results. That said, we understand every hiring process is unique, and therefore also provide breadth and depth in our configurations, with features like custom fields, screening questions, analytics, reporting and more, for customers to decide what is most necessary - just as the GDPR allows them to do - the personal data they deem absolutely necessary to their hiring process and to demonstrate compliance thereof.

While Data Controllers are given authority to determine what personal data is necessary for achieving the specified purpose of their data processing activity, this means they also carry the burden of proof in the event of an alleged GDPR violation or audit to show their data processing activities are limited only to that personal data that is necessary.

PRINCIPLE 4 - “CURRENT AND ACCURATE” — The GDPR states that Data Controllers must take “every reasonable step” for ensuring the personal data processed is **current and accurate**. This principle is really self-explanatory and simply means data must be up-to-date and correct as to its purpose. Where inaccuracies exist, the Data Controller is responsible for remedying the errors without delay, and the erroneous information must be “erased or rectified” per the GDPR.

A common risk arising in recruitment is the presence of an outdated talent database, which runs directly afoul of this accuracy rule. Hence, personal data collected from your applicants must be accurate and up-to-date. Where it isn't, your candidates (Data Subjects) have the “right to rectification,” compelling YOU (the Data Controller) to remedy any inaccuracies. Managing information accuracy is an incredibly onerous and burdensome process, so having a recruitment solution that helps mitigate this risk is key.

 SmartRecruiters supports our customers in their efforts to capture accurate information by offering functionality that serves to reduce the risk of erroneous and duplicative data. SmartRecruiters features like Live Profiles and Profile Merger, or our seamless HRIS integrations - that offer integration capability to all major HRIS providers - promote current, credible, and accurate candidate data maintenance for our customers.

PRINCIPLE 5 - “LIMITED RETENTION” — Personal data may not be retained indefinitely, so data retention limits must apply. The GDPR makes it clear that personal data may be retained “**for only as long as is necessary,**” when in a format where the data subject can be readily identified. Further, personal data must be processed in a manner that ensures the security of the data, while also enabling the data subject to exercise his/her rights under the GDPR. While this discussion only highlights data subjects' rights, for those who want to learn more, please reference the box below: The Rights of Data Subjects.



Five Key Principles for Processing Personal Data: A Checklist

- Fair and lawful with transparency
- Explicitly specified
- Only what is necessary
- Current and accurate
- Limited Retention




The Rights of Data Subjects

- » Right to Information
- » Right of Access
- » Right of Rectification
- » Right to Erasure
- » Right to Receive Info within 1-month
- » Right to Restrict Processing
- » Notification of 3rd Parties
- » Right to Data Portability
- » The Right to Object
- » The Right Not to Be Evaluated
- » The Right to Bring Class-Actions

 **Where Can I Learn More** → *GDPR, Chapter 3: Rights of Data Subjects, Articles 12 through Article 23 GDPR recitals: 58 through 73*

So, how long is too long? The GDPR does not currently specify a length of time, as it likely depends on the nature of the data processing activity, and/or local requirements. That said, the burden is on the Data Controller to show adequate data retention limits exist and that such limits are followed. Thus, an important question for Data Controllers to consider, especially if relying on an outside Data Processors, is how this will be accomplished.

 SmartRecruiters platform is designed with embedded features to assist customers with meeting their compliance needs. Specific to retention of applicant data, SmartRecruiters provides a simple and easy-to-use Compliance Administration interface that enables customers to set their own rules and limits for maintaining an applicant's personal data. While our platform certainly aids customers in facilitating compliance with data retention regulations, the burden ultimately lies on the customer for ensuring and providing proof of actual compliance.

As we briefly alluded to above in Principle 5, the GDPR makes clear the ultimate responsibility for ensuring data processing activities are compliant rests on the Data Controller. Thus, the Data Controller (meaning YOU, the customer) bears the burden for demonstrating that each of these principles (#1-5) are satisfied with respect to your data processing activities. To ensure your team is compliant, we recommend a thorough review of each of these within the GDPR.

 **Where Can I Learn More** → *GDPR, Chapter 2: Principles, Article 5*



Data Processing Obligations

Previously, under the DPR, data processing obligations were primarily the responsibility of the Data Controller, only. This has changed under the new GDPR, which now applies to both Data Controllers and Data Processors. Each have separate obligations that must be met to be compliant in the processing of personal data. As such, we recommend familiarizing your organization with Chapter 4 of the GDPR and accompanying recitals, which speak to these obligations. Below, we've provided a high-level summary as a guideline for you and your team to get organized.

SmartRecruiters Customers - Your Obligations under the GDPR

As discussed earlier in this paper, a Data Controller is the entity that determines what personal data of a data subject, is processed. At SmartRecruiters our customers - meaning YOU - are the Data Controller because you decide what data to collect from job applicants, leveraging our platform, that is necessary for qualifying, evaluating, and hiring candidates who participate in your recruitment processes. **As such, our customers are responsible for demonstrating the following under the GDPR:**

- » Compliance with GDPR Data Protection Principles (Referenced above in Section 4 of this paper)
- » Incorporates 'Privacy by Design'
 - Compliance measures are a standard considered of both the planning and implementing of any new product or service that involves data processing activities. In other words, always be thinking “Does this help facilitate compliance?” (e.g. implementing a product like SmartRecruiters, which provides features to enable compliance in your hiring process)
- » Minimum Amount of Personal Data Processed
- » Data Protection Officer Appointed (to the extent GDPR required)
- » Written Data Processing Agreement for Data Processors
- » Maintain Proper Records of Data Processing Activities
- » Report Data Breaches without Undue Delay (within 72hrs)
- » Notify Data Subjects of Breaches without Delay

 [Where Can I Learn More](#) → *GDPR, Chapter 4: Controller & Processes, Section 1: General Obligations, Art 22 through Art 43*



SmartRecruiters Obligations under the GDPR

According to the GDPR, and as discussed previously, SmartRecruiters is a Data Processor, meaning we process personal data (job applicants) on behalf of a data controller (YOU). Although different from data controllers, data processors also have obligations under the GDPR. As such, SmartRecruiters is responsible for the following under the GDPR:

- » Acts on the Data Controllers Written Instructions (generally in the form of a contract know as a DPA or Data Processing Agreement)
- » Imposes Confidentiality on Personnel Processing Data
- » Ensure Confidentiality of Data Processing Activities
- » Implements Measures to Assist Data Controllers with Compliance
- » Return or Destroy Personal Data at Data Controller's Election or Contract End
- » Provide Data Controller the Information Necessary to Demonstrate GDPR Compliance
- » Sub-Processors Appointed Only with Permission from Data Controller
- » Maintain records of data processing activity, available on request
- » Appoint Data Privacy Officer (to the extent required under the GDPR)
- » Implement measures for data security and data protection
- » Appropriate measures for cross-border data transfers



Many Data Processors meet these obligations through the existence of a written data processing agreement (DPA). SmartRecruiters is no exception - a data processing agreement is a formality that is executed between SmartRecruiters and our customers as part of our GDPR compliance obligations. In addition, SmartRecruiters also executes DPAs with our sub processors to provide additional protections. Specific to our customer DPA, this agreement is reviewed, agreed upon and executed with our customers at contract signing and immediately prior to implementation getting underway.

That said, the GDPR ultimately imposes the duty of care on the Data Controller for selecting a Data Processor who can appropriately assist and facilitate compliance with GDPR principles.

 [Where Can I Learn More](#) → *GDPR, Chapter 4: Controller & Processes, Section 1: General Obligations, Art 22 through Art 43*



The Future of Global Compliance



If you'd like more information about the SmartRecruiters platform, or specifically any of our built-in compliance enabling features mentioned in this paper, we'd love to speak with you.

Email us at :
sales@smartrecruiters.com

Suffice to say, the GDPR has implemented a complete overhaul of the former provisions of the now expired Data Protection Directive in an effort to provide appropriate protections for data subjects with respect to how organizations process, transfer, store, and protect the enormous amount of data available in this new digital world. Therefore, it is important that when your organization selects a product, tool, or software specific to your recruiting and hiring process, that your selection entails consideration of these new compliance obligations. Remember the old "Privacy by Design" rule mentioned above?

And while there is still some uncertainty and ambiguity as to how these provisions will be enforced and interpreted once this measure takes full effect in May 2018, especially in light of recent political events like Brexit - referencing the UK's departure from the European Union,

data privacy considerations and conversations around the processing of personal data should not be delayed.

At SmartRecruiters, we believe hiring is success, which starts and ends with great people. And while committed to helping our customers propel their businesses forward by connecting them with great talent - we are also extremely sensitive to protecting the incredible amount of data that is generated from your hiring activities. As such, we hope this guide provides you some insights for taking a proactive approach to data privacy, specific to your recruitment data processing activities. And while this may seem incredibly overwhelming, here at SmartRecruiters, we are committed to helping our customers meet compliance objectives wherever their hiring activities take place.



SmartRecruiters' Talent Acquisition Suite is used by high-performance organizations for making the best hires. It has full functionality for recruitment marketing and collaborative hiring built on a modern cloud platform.

For more information, follow us at [@SmartRecruiters](#), on LinkedIn or visit us at [smartrecruiters.com](#).