



Achieving GDPR Compliance with Avature



What You Need to Know About GDPR

The General Data Protection Regulation, or GDPR, is a regulation that was passed by the European Union in 2016 to update and replace the EU Data Protection Directive of 1995. GDPR harmonizes data protection regulations across EU member countries. However, the new regulation also applies to all foreign companies processing the data of individuals in the EU, even if the companies do not have an established place of business inside the EU. Furthermore, GDPR introduces large penalties for non-compliance. GDPR presents some new challenges for non-EU companies — not the least of which being that they must be compliant by May 25, 2018.

In order to be in compliance, companies will need to:

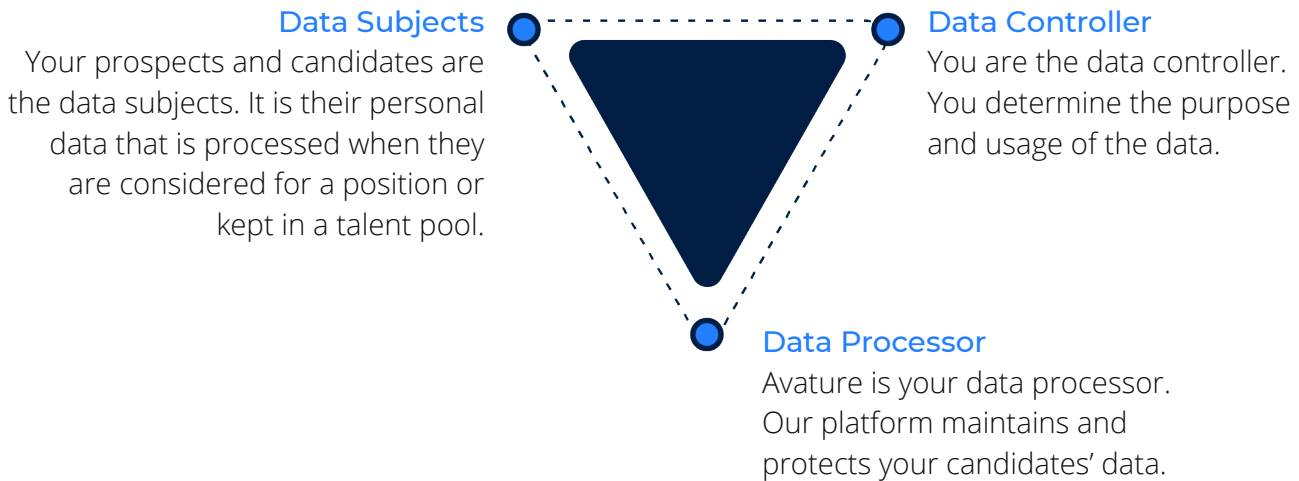
- Be familiar with the GDPR guiding principles
- Establish business processes that are designed to support those principles
- Process personal data legally and ensure their data processor provides adequate technical controls

Recruiting and marketing programs, which depend on collecting and using personal data, face one of the biggest challenges. It is important to remember that the EU definition of personal data is broad.

“Fortunately, GDPR simplifies EU data protection regulations,” says Beatriz Quintana, Chief Privacy Officer of Avature, “replacing a more fragmented legislation, which was essentially a framework with different implementations depending upon the EU country. Complying with data privacy laws under GDPR will be more homogeneous.”

Impacted Parties

Generally, GDPR oversees three groups that either have personal data rights or personal data obligations. When working with Avature, these are:



Guiding Principles

In order to be prepared for GDPR, your company must comply with the following principles.

Fair and lawful: You must have legitimate grounds for collecting a person's data, and you are required to provide full transparency about how you will use candidates' data.

For explicitly specified purpose: You must only use your candidates' personal data for the purpose you originally said it would be used.

Only what is needed: The data you hold on your candidates must be adequate for the defined purpose. Privacy notices must be clearer than before, and candidates must be able to withdraw consent at any time.

Accurate and updated: You must regularly take steps to keep candidates' personal information up to date.

Limited retention: You must regularly review the length of time you hold onto candidates' data. Data that is out of date or no longer necessary must be properly destroyed or deleted.

Penalties

Under GDPR, people have enhanced rights to access the information that companies have about them, and businesses have new obligations for data management. Noncompliant companies may be charged penalties of up to 4% of worldwide turnover or €20 million, whichever is greater.

The €20 Million Question

Can recruiting programs comply with GDPR and remain effective?

The short answer is yes.

Avature has been helping EU customers comply with the EU Data Protection Directive for the past 10 years. Our customers — which include large and small EU companies, all the major global consulting companies, many of the largest banks and manufactures in the UK and Germany, and several EU government entities — have developed competitive recruiting programs that operate effectively within the EU and meet the data regulations.

If you still haven't done anything to comply with GDPR, you need to move quickly because, as with many of our non- EU customers, you may need to make significant changes to the way you process personal data.

The good news is that Avature can be configured to support GDPR-compliant recruitment marketing programs.

Avature's security and privacy controls meet the highest standards and are ISO 27001 and SOC 2 certified. Our controls have passed multiple onsite audits and penetration tests.

Avature – Your Data Processing Partner

Leveraging our fundamental focus on configuration, we have invested in technical functionality specifically designed to support privacy laws. Our system is highly configurable, and you can determine how to process data in the manner that is legally compliant.*

We have also assisted customers in their response to government inquiries relating to individual citizens' privacy complaints and supported customers in their successful resolution of complaints. Our legal team knows how to draft, review, and execute amendments to existing data protection agreements.

Support & Security Measures

Our main responsibilities as a data processor are to provide for the confidentiality, integrity, availability, and resilience of your data. Behind the user interface, we implement technical and organizational security measures such as:

- Firewall, encryption, and other technologies to protect the data
- Separation of processing for different customers and their different purposes
- Role segregation so that only Avature employees who need to access your data are able to view it.

Avature's online documentation (Help & News), available from within your instance, describes in detail how all of our features work.

* While Avature offers functionalities to support compliant processes, we are not a law firm and do not provide legal advice. We have, however, worked directly with the legal departments of major organizations and their recruiting teams to implement compliant recruiting programs. Avature's consultants have supported the implementation of many recruiting programs for EU customers, following their requirements in accordance with EU privacy laws. We strongly recommend you consult with your legal counsel to decide upon compliance processes.

Features

The Avature platform is designed for configurability. So when compliance regulations change, our technology can keep pace.

Specific to GDPR, our solutions offer different features to help you achieve compliance.

Customizable opt-in/out or double opt-in workflows that automate the consent process and regularly re-evaluate candidate consent

Automated purging or deletion of data at intervals determined by you

Encryption: that keeps confidential data accessible/editable on a need-to-know basis

Configurable security settings: for your users in accordance with your security needs

Full audit journal: to trace interactions with candidates, including consents, updates and changes

Unsubscribe links: in emails sent through Avature so candidates can choose to opt-out

Consent forms: to manage and keep track of individuals' consent with timestamps

With GDPR coming into effect, if your legal counsel advises you to reconfigure your instance, please contact your sales representative and our consultants will support any reconfiguration according to your instructions. For more information, contact your sales representative or email sales@avature.net.

Other Privacy Policy Updates

Many of our customers operate in China. Our configurability enables you to tailor the solution to your unique processes in that region.

China's Information Security Technology - Personal Information Security Specification became effective May 1, 2018. The standard sets out data protection concepts and principles for key laws and regulations, such as the China Cybersecurity Law. Avature's configurable system can support you in complying with these provisions.