



SmartRecruiters

Data Privacy & Government Surveillance Frequently Asked Questions

SmartRecruiters is committed to complying with all applicable laws governing the privacy, security, and treatment of its customers' data. This includes existing and emerging laws in the United States, European Union, and other jurisdictions. Because these may vary across countries, SmartRecruiters has prepared these Frequently Asked Questions (“FAQs”) addressing common data privacy inquiries from our international customers and partners.

FAQ 1 – Does SmartRecruiters comply with the GDPR and other data privacy protection laws?

- SmartRecruiters complies with the local data privacy laws in each of the countries where we operate. Our internal policies are designed to protect our customers' data in accordance with the local data privacy laws in the countries where their data is actually stored. This includes complying with the GDPR if customer data is subject to the GDPR. For more information, please see SmartRecruiters' Privacy Policy.

FAQ 2 – Where does SmartRecruiters store European customers' data?

- SmartRecruiters stores all European customers' data on servers that are in the European Economic Area (EEA), which is governed by GDPR. SmartRecruiters complies with the local data privacy laws, including GDPR, in each of the countries where customers' data are stored.

FAQ 3 – Does SmartRecruiters transfer European customers' data to recipients in the U.S.?

- Except if a European Customer uses SMS messaging, then if a customer requests that SmartRecruiters not provide support from the United States, SmartRecruiters does not transfer European customers' data to a recipient in the U.S. for processing either by SmartRecruiters itself or by any other data processor, and European customers' data remains in the EEA. SmartRecruiters uses a limited number of third-party providers in the EEA for data processing (and one in the United States should a customer choose to use SMS messaging), customer support, hosting, certain feature/functionality, and technical operations. SmartRecruiters ensures that all personal data is handled, processed, transferred, and stored in accordance with GDPR, including with the use of the latest



SmartRecruiters

Data Privacy & Government Surveillance Frequently Asked Questions

Standard Contractual Clauses that the European Commission has approved for ensuring appropriate data protection safeguards. For more information, please see SmartRecruiters' Privacy Policy.

FAQ 4 – Does SmartRecruiters use encryption to protect European customers' data?

- Yes, SmartRecruiters encrypts all customer data both as data are stored on servers (i.e., at rest) and data they are transferred (i.e., in transit) to another entity.

FAQ 5 – Does Executive Order 12333 require SmartRecruiters to participate in U.S. Government surveillance activities?

- Executive Order 12,333 governs the U.S. intelligence community's foreign surveillance and collection activities. It does not authorize intelligence collection against U.S.-based targets or require U.S. companies like SmartRecruiters to participate in intelligence gathering. SmartRecruiters has no role in or control over any U.S. intelligence community activities.

FAQ 6 – Does the Foreign Intelligence Surveillance Act ("FISA") require SmartRecruiters to participate in U.S. Government surveillance activities?

- FISA is designed to investigate foreign spies and terrorist organizations operating within the United States. The U.S. Government can only obtain information under FISA through a warrant issued by an independent federal court. SmartRecruiters has not received such warrants, does not anticipate receiving any such warrants, and reserves the right to challenge them through juridical means when necessary.

FAQ 7 – Does Section 702 of FISA apply to SmartRecruiters?

- Section 702 of FISA authorizes the U.S. government to apply to an independent federal court for a warrant to collect communications from electronic communications or internet service providers the purpose of investigating foreign spies and terrorist organizations. SmartRecruiters is not an electronic communications or internet service provider and has



SmartRecruiters

Data Privacy & Government Surveillance Frequently Asked Questions

never received a Section 702 warrant. In addition, based on [public authorities](#) and SmartRecruiters' experience, the personal data that SmartRecruiters maintains is highly unlikely to be of any interest to U.S. foreign intelligence investigation.

- Consistent with the EDPB's recent [recommendations](#) on measures that supplement transfer tools, SmartRecruiters has based this assessment on its own documented practical experiences, public statements issued by the U.S. government, the documented experiences of other actors that process similar personal data, and publicly reported cases evidencing the past application of U.S. national security laws, including FISA Section 702. Furthermore, as the U.S. Department of Justice, the Office of the Director of National Intelligence, and the Department of Commerce made clear in a joint [White Paper](#) issued in September 2020, companies like SmartRecruiters that offer "ordinary commercial products or services," and whose data transfers "involve ordinary commercial information like employee, customer, or sales records," have "no basis to believe U.S. intelligence agencies would seek to collect that data" through FISA Section 702¹.

FAQ 8 – Does the USA PATRIOT Act and its successor laws require SmartRecruiters to participate in U.S. Government surveillance activities?

- These laws are designed to investigate money laundering and terrorist financing. Collecting information under these laws typically requires a court order, geographic targeting order, or national security letter. SmartRecruiters has not received such orders, does not anticipate receiving any such orders, and reserves the right to challenge them through juridical means when necessary. Based on [public authorities](#), the type of personal data that our customers generally collect and place into SmartRecruiters' software is not of interest to U.S. intelligence agencies.

FAQ 9 – Does SmartRecruiters voluntarily participate in any U.S. Government or surveillance programs, including those administered by the National Security Agency ("NSA")?

¹ Cf. page 2 of the White Paper.



SmartRecruiters

Data Privacy & Government Surveillance Frequently Asked Questions

- SmartRecruiters does not knowingly or voluntarily participate in any U.S. Government intelligence or surveillance programs, including surveillance and data collection programs administered by the NSA.

FAQ 10 – Does SmartRecruiters provide any customer data to any intelligence agencies?

- SmartRecruiters does not voluntarily provide customer data with any U.S. or foreign intelligence agencies. Obtaining access to U.S.-based customer data would require a court order or similar directive under U.S. law. SmartRecruiters has never received, and does not anticipate receiving, such an order in connection with intelligence activities.

FAQ 11 – Does SmartRecruiters provide metadata or other similar content to U.S. intelligence agencies?

- SmartRecruiters does not provide customer metadata to any intelligence agencies or participate in any government programs involving the bulk collection of metadata. Obtaining access to U.S.-based customer metadata typically requires a court order under U.S. law. SmartRecruiters has never received, and does not anticipate receiving, such an order in connection with intelligence activities.

FAQ 12 – Does SmartRecruiters share customer data stored outside the United States with any U.S. intelligence agencies?

- SmartRecruiters' customers control how and where their data is stored and shared. We do not relocate customer data unless a customer specifically directs us to do so, and such activities are authorized under local privacy laws. Nor do we share customer data with any government agency unless we are required to do so under applicable local laws.

FAQ 13 – Does SmartRecruiters build any “backdoors” into its software, source code, or systems that would allow U.S. intelligence agencies to access customer data?



SmartRecruiters

Data Privacy & Government Surveillance Frequently Asked Questions

- SmartRecruiters is committed to protecting the privacy and security of its customer's data, regardless of where that data is located. We do not provide any government agencies with software source code, encryption keys, or other forms of access for the purpose of accessing customer data. SmartRecruiters has never received, and does not anticipate receiving, requests for "backdoor" access to its software and systems.

FAQ 14 – Does SmartRecruiters work with any vendors, suppliers, or other business partners that participate in intelligence and surveillance programs?

- SmartRecruiters' business partners are commercial enterprises. As such, we are not aware of any vendors or suppliers participating in such programs. Even if our business partners were engaged in such activities, however, our systems are designed to prevent them from accessing customer data without the customer's prior authorization. As noted, SmartRecruiters uses encryption for data at rest and in transit and uses Standard Contractual Clauses that the European Commission has approved for ensuring appropriate data protection safeguards.

FAQ 15 – Is SmartRecruiters subject to any other laws that would allow governments access to customer data?

- Like any company, SmartRecruiters is subject to the local laws that apply in the countries where it stores customer data. This means that SmartRecruiters may occasionally need to comply with court orders, subpoenas, or search warrants related to routine law enforcement activities. Such measures are consistent with the GDPR's longstanding law enforcement exceptions.

FAQ 16 – How will SmartRecruiters protect customer data during law enforcement investigations?

- SmartRecruiters believes that any government request should be directed to the appropriate SmartRecruiters customer that owns the data.



SmartRecruiters

Data Privacy & Government Surveillance Frequently Asked Questions

- SmartRecruiters will work with its legal advisors to determine whether court orders, subpoenas, or other agency directives are authorized under the relevant national laws. If such orders are not consistent with applicable local law, then SmartRecruiters reserves the right to challenge them through judicial action or other means.
- If SmartRecruiters receives a government request for customer data, SmartRecruiters will investigate: (1) whether SmartRecruiters can seek interim measures to suspend enforcement of the government request until SmartRecruiters' challenge has been resolved; (2) whether (a) applicable law prohibits SmartRecruiters from notifying the affected customer of the government request prior to producing the requested information, and if not, such notice will include all relevant information that SmartRecruiters is legally permitted to provide to the customer, and (b) if a government request purports to require SmartRecruiters to delay customer notice indefinitely, whether SmartRecruiters can challenge it; and (3) whether, if a law enforcement or government agency contacts SmartRecruiters, SmartRecruiters can inform the agency that it is merely a processor of its customers' data, and redirect the agency to make the request directly to the relevant customer.