ADC Membership Application

Online Application Form

Company Name

Form Submitter

Regulated Entity

Regulating Authority

Does your organization have the technical capability, willingness, resources, time, and staff available to execute projects if awarded any such contracts in the future?

Are there any 3rd-party dependencies/access restrictions to the data/services that would impact our receipt and/or use of the data or services (e.g. expiration of upstream license, agreement, changing privacy regulations like CPRA).

Do you collect or generate the data or services yourself, or do you buy or collect the data or Services from others?

Are there physical and/or virtual controls in place to protect the systems and locations where your data is stored?

Has your company confirmed that the people or organizations providing the data or services in your offerings have the legal right to do so?

If any information is shared with external parties outside of your organization, has your company ensured that all agreements, contracts, and laws under which sharing can occur are being complied with properly?

Does the data or services contain or are derived from any information that is otherwise confidential? (e.g. your license to the data is covered by an NDA).

Has the company used reasonable best efforts to determine that any data you use to create the data or services is not derived from nor contains information related to a breach of fiduciary duty, breach of contract, or deceptive behaviors?

Is covered personal information collected by the company (or any third-party sources of any underlying data) or used by the company to produce the data as part of its products and/or services?

Does the company maintain written policies and procedures regarding the handling of any sensitive information (e.g. covered personal information, confidential information, data supplier due diligence) and have proper controls in place to ensure that those policies and procedures are adhered to?

If applicable, does the company attest that it complies with the terms of use of any data source from which data is obtained (e.g. websites, third party suppliers, etc.)?

Does the company have an internal legal department or use outside counsel specifically relating to data and/or the companies data practices more generally (Does not apply to employment lawyers or non-related legal help) To ensure the legal and compliance aspects of the collection and dissemination of data are managed by the company in a proper manner that is up to date with current standards?

In the last five years, has the company ever experienced any negative scenarios related to the company's data collection/use/distribution practices or related to the providers of the underlying data used by your company?

Does the company have an individual or internal group in place who are responsible for the organization's information security?

Does the company attest that the data or services offered will be clean and free from any cyber security related threats and that reasonable protections are in place to avoid any future threats? (e.g. Use of firewalls, scanning, tier certificates, etc.)

Does the company have any of the following actions and policies in place to mitigate and proactively prepare for any risks? Please select all that apply:

- [ ] Internal audits to ensure compliance with risk mitigating policies that occur at standard frequency
- [ ] Periodic review of policies to update with the most recent developments Business liability insurance policy
- [ ] Disaster recovery plan
- [ ] Data retention policy; including backup data
- [ ] Business continuity plan
- [ ] Incident response plan
- [ ] Security threat detection/management plan
- [ ] Vulnerability/patch management plan or process
- [ ] Virus prevention plan or process
- [ ] Use of various authentication methods E timed lockouts, password requirements, smart cards, tokens, two factor authentication, etc.)