

**Policy brief & purpose**

The Think To DO Institute **Data Protection Policy** refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

**Scope** This policy refers to all parties (employees, job candidates, customers, research subjects, suppliers etc.) who provide any amount of information to us.

**Who is covered under the Data Protection Policy?** Employees, volunteer dynamic thinkers, and its collaborators must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data. **Policy elements** As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

The Think To DO Institute collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data, the Think To DO Institute has direct obligations towards people to whom the data belongs. Specifically, we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

**Actions**

To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from [cyberattacks](#)
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data

- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Our data protection provisions will appear on our website.

The policy including this statement will appear in the link from the opt-in statement to the website:  
All emails include an unsubscribe link. You may opt-out at any time. See our [Privacy Policy](#).

**Your rights:**

Your rights include:

- Request the personal data we hold about you. This may be subject to a fixed fee of 20NAF
- Complain to a supervisory authority if you believe we have misused your data
- Withdraw consent

### **International information transfers**

We use trusted companies to process data outside the European Economic Area. We keep shared data to the minimum necessary, review the privacy policies of those companies and only work with companies we trust to keep your data safe.

### **Amendments**

We review and update our privacy policy from time to time. We may notify you of updates by email. December 2020.

### **Contact information and controller**

If you have any requests concerning your personal information or any queries with regard to these practices, please contact the Data Protection Officer from our website: [contact@thinktodoinstitute.com](mailto:contact@thinktodoinstitute.com)

### **Survey Data Controls**

Very clear consent language will be placed upfront in each survey or collection point as well as opt-in language to ensure people that the survey has contacted have consented. Also, at the top of the funnel, a check-box or other opt-in mechanism is present.

A clear statement will be made for people who have opted in and consented to change their minds and how they can unsubscribe. Every marketing or solicitation type of email or communication connected to the survey needs to include these provisions.

The access controls on the data are auditable and the data is stored in a manner that if a complaint arises around misuse, the think tank can provide evidence and details around the use of the data (like a traceability matrix). If this means setting up a customer database and segregated zones for each type of data, this will be done.

### **Disciplinary Consequences**

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.