Data Protection Policy

Introduction

This policy refers to all data collected from employees, candidates, users, customers, vendors, or other parties that provide information to Reveal.

Reveal employees must follow this policy. Contractors, consultants, partners and any other external entities are also covered. Generally, our policy refers to anyone we collaborate with or who acts on our behalf and may need access to Reveal data.

Data Protection Policy

As part of our operations, we obtain and process information, some of which can be used to identify individuals (personally-identifiable information, or PII).

Our company 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.

The data will be:

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

The data will not be:

- Communicated informally
- Stored for more than the amount of time specified in our Terms of Service, Privacy Policy, customer contracts, or other binding agreements
- Downloaded to unapproved devices
- 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, Reveal 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 within legal guidelines specified by company policies or law-enforcement agencies

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.)

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Reveal management will determine how serious an employee's offense is and take the appropriate action.

Further Questions and Responsibility

Any questions regarding the use of or suggested modifications to Non-Disclosure Agreements should be referred to the CTO.

It is the CTO's responsibility for ensuring this policy is followed.

Last updated: *2021-10-07*