5 Prime Sciences data protection policy

Policy brief & purpose

Our **5 Prime Sciences Data Protection Policy** refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality. Since 5 Prime Sciences handles sensitive medical data, which includes genetic information, we consider Data Protection to be a fundamental objective of our mission.

To fulfil this objective we have written this policy to ensure that we gather, store and handle data fairly and transparently.

Scope

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

Who is covered under the Data Protection Policy?

Employees of our company and its subsidiaries 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 access to data. Data is never granted to a third-party without explicit written permission of the data owner.

Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that is subject to a Business Contract, a Material or Data Transfer Agreement, or any other signed agreement that requires a data security policy.

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.

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 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 company has direct obligations towards the owner to whom the data belongs. To exercise data protection we're committed to:

- Encrypt the data at rest or in transit using industry standards.
- Strictly avoid storing individual level data on offline devices.
- Restrict and monitor access to sensitive data.
- Apply transparent data collection procedures.
- Regularly train and validate that employees are up-to-date in online privacy and security measures, including the use of secure authentication (strong passwords, password managers, multi-factor authentication) and disk encryption of offline data.
- Build secure applications 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 Consequences

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