Data Privacy Code of Conduct

The right to privacy is a fundamental human right.
The protection and responsible use of personal data is reflected in our daily operations.
Starkdata sees data as a driver for business excellence. As such, we strive to the preferred partner to all who may provide such data.

We are committed to collecting and using data in a lawful, fair, legitimate and ethical way, and will always respect the privacy of individuals in order to earn and deserve their trust.
Starkdata assumes accountability for the compliant processing of personal data by itself or by its trusted service and cooperation partners.

Any information related to an identified or identifiable person must be collected and processed in compliance with applicable data privacy laws (e.g. Swiss Federal Act on Data Protection, EU General Data Protection Regulation and the US Health Insurance Portability and Accountability Act).

The applicable regulation for each project is determined by geographic location of project and project Parties. (e.g Projects within EU are submitted to the full regulation of GDPR)

Starkdata employees with access to such personal data are expected to apply the privacy principles of lawful, fair and transparent data processing, respecting any purpose limitations, as well as the principles of data minimisation, accuracy, storage limitation, integrity and confidentiality.

Contractors, and any third-party processors that might engage to process personal data on Starkdata's behalf are also bound to the rules of the present Code, and the same regulations and applicable laws.

Starkdata will request evidence to any contractors, and any third-party processors processing data on Starkdata's behalf, of their compliance with this Code, laws and applicable regulations.

Starkdata will also oversee contractors, and any third-party processors data processing actions through regular supervision and audits.

Personal data means all information relating to an identified or identifiable person. An identifiable person is identifiable, directly or indirectly, by reference to an identifier, which may be the name, identification number, location data (IP address), electronic identifiers (e-mail) or to one or more specific elements of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

There is also a category of special data, those that reveal racial or ethnic origin, opinions, religious or philosophical beliefs, or trade union membership, as well as the treatment of genetic data, biometric data to identify a person unambiguously, health data or data relating to a person's sexual life or sexual orientation.

The data falling in this category is not collected by Starkdata unless their treatment finds specific grounds in law and is critical for a legitimate purpose (e.g medical research data for a specific public interest project).

In case of doubt about the application of any regulations and the rules set forth in this Code, all employees, contractors, subcontractors, third-parties and customers should contact the Compliance Officer in order to clarify any doubts as quickly as possible.

Whenever clarifications are required, the Compliance Officer should document the doubts and questions.

To all omissions in this Code will be applied the applicable laws of Data Protection and Privacy following the same rule of jurisdiction determined above.

1. Fairness and transparency

1 - Starkdata will be fair and transparent in the processing of personal data.

2 - Whenever collecting personal data, Starkdata will:

(i) Obtain data subjects' consent.

(ii) Provide clear and concise information to data subjects about how collection, use, and sharing of personal data takes place.

(iii) Ensure the data subjects' rights and privacy are protected.

2. Legitimate interests

1 - Starkdata will only process personal data for legitimate interests and will balance those interests against the rights and freedoms of data subjects.

2 - Legitimate interests for personal data collection are determined within the scope of applicable data privacy and protection regulations.

3. Collection of personal data

1 - Starkdata will only collect personal data that is necessary for legitimate specific purposes.

2 - Starkdata will not collect more personal data than necessary and will not collect personal data that is not relevant to those purposes.

3 - Each project is to be submitted to impact and data assessments, and a compliance report should be carried out determining categories of data being used, the reason for collection of said categories in the context of the project, mentioning specifically the legitimate interests that enable collection, use and processing of data categories, along with identified risks, mitigation actions and auditing processes to ensure data privacy and data protection, along with additional compliance rules applicable.

4 – Impact and data assessments carried out internally should follow the compliance guidelines for data processing and privacy along with the relevant additional regulations, according to the scope, applicable industry, and type of use of our technology.

5 - Personal information should be treated according to some rules, namely:

(i) Always taking into account a specific and legitimate purpose;

(ii) On the basis of a contractual and confidential relationship with the data subject;

(iii) With the written consent of the holders of personal data;

(iv) With the detail that is legally possible or required, according to the diversity of situations.

4.Anonymisation

Starkdata will always anonymise personal data. Identifiable personal data is anonymized by hashing with salt. This allows for stored data to be non-identifiable at rest. For external identification, we use randomized unique universal Ids, which guarantees full anonymity and no relation with the personal data. In transit data is always encrypted according to industry standards using TLS 1.3.

5.Information to data subjects

1 – Starkdata acts mostly as Data Processor Company for Data Controllers and/or Data Owners who are typically enterprises or legal entities.

2 - Whenever processing data from customers, users, patients or equivalent as a Data Processing Company for Data Controllers and/or Data Owners, Starkdata ensures information to data subjects through the scope of its Project Documents that include but are not necessarily limited to Architecture Documents, Risk Assessment Reports, Impact Assessment Report, Privacy and Compliance Policies, Data Processing Agreements.

3 - Whenever collecting data directly from data subjects, Starkdata will provide data subjects with information about how processing of their personal data is carried out, including the purposes of processing, the categories of personal data processed, and eventual recipients of the personal data.

4 - Under no circumstances will Starkdata share any personal data with third parties outside of a specific project scope and whenever said data sharing is critical to project scope or goals.

6.Data subjects' rights

Starkdata will respect the rights of data subjects under the GDPR, SFADA or HIPAA, including the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, and the right to object.

7.Transfer of personal data to third countries

If Starkdata for any legitimate reason, as defined by data protection and privacy policies and regulations, needs to transfer personal data to a third country, will take appropriate safeguards to ensure that the personal data is protected in accordance with the GDPR, SFADA or HIPAA, and any additional data privacy and protection regulations applicable.

8. Security of processing

Starkdata will implement appropriate technical and organizational measures to ensure the security of personal data. This includes protecting personal data from unauthorized access, use, disclosure, or destruction.

9.Employees working with personal data

All employees who treat personal data are bound by professional confidentiality and are prohibited of disclosing or using such data for other purposes. Exceptions are made in cases where the law requires the transmission of data, particularly when required by authorities, and only in the strict field in which it is required. These employees have an increased responsibility for the security of personal data of clients and other employees.

For the safeguard of confidentiality employees are bound by strict Non-Disclosure Agreements.

10.Compliance Officer

1 - Starkdata has an internal Compliance Officer to ensure compliance with the Data Protection Regulations, amongst other applicable regulations.

2 - The responsibility of Compliance falls under the Operations Department and is currently led by Catarina Nunes, who can be contacted to clarify any question regarding data privacy, compliance and related through the address compliance@starkdata.ai.

3 – Starkdata's Compliance Officer is committed to implementing the necessary measures to ensure that personal data is protected, as well as the obligation to continuously update data security measures.

4 - The Compliance Officer main focus is compliance within impartial, and no conflicts of interest performance.

5 - The Compliance Officer is also responsible for identifying risks and suggesting opportunities for improvement related to the Data Protection Policy.

11. Data Breach

In the unlikely scenario of a data breach, a notification should be made to the Compliance Officer.

After a thorough review of the notification, the Compliance Officer shall communicate the situation to the National Data Protection Commission, hereinafter NDPC, within a maximum of 72 hours.

The decision to notify the violation to NDPC is the responsibility of the Compliance Officer and the management, who will make a case-by-case analysis to understand the type of violation, the risks and associated consequences and the measures to be taken.

12. Information and Training of Employees working with data

All information related to the data privacy regulations and applicable laws, along with the measures to be taken to comply with them, are made available to employees.

It is the Compliance Officer's responsibility to provide adequate training to internal teams within the scope of data protection and privacy laws applicable.

13. Monitoring

1- Starkdata will monitor compliance with the present Code , regularly, conducting internal audits every six months, or more frequently, according to specific identified needs. Starkdata will also conduct audits and reviews of internal data processing practices ensuring compliance with the GDPR, SFADA or HIPAA, and any applicable additional data protection and data privacy regulations.

2 - Any change to the method of collection and processing of personal data should be reported to the Compliance Officer to verify its feasibility and compliance with the applicable standards, and then inform the data holder.

14. Complaints

If a data subject has a complaint about how Starkdata processes their personal data, Starkdata will investigate the complaint and take appropriate action.

15. Dispute resolution

If Starkdata and a data subject are unable to resolve a dispute about processing of their personal data, Starkdata will offer to use an alternative dispute resolution procedure, such as mediation or arbitration.

16. Additional measures of security

Employees must use any computer resources made available to them exclusively for professional purposes and diligently taking care of its maintenance.

Computer resources made available for employees are only for professional use and is it strictly forbidden to be used outside of professional context.

Internal Starkdata's files, software available, data and any other resources property of Starkdata can only be accessed by specifically authorized equipment, previously validated and prepared by Starkdata.

Starkdata implemented security measures throughout the organization, namely through the creation of files and databases of data with restricted access, so that personal data do not suffer any violation, disclosure or misuse.

To protect the information customers provide Starkdata, we have implemented various security measures, including administrative, technical and physical measures.

Starkdata also adopts other security measures regarding the security of personal data:
(i) Antivirus software that provides protection against malware.
(ii) The Wi-Fi network supports strong encryption protocols
(iii) Remote access to our corporate network is only possible through a VPN (Virtual Private Network).
(iv) Privileged accounts are not used for daily tasks and access to them is possible only by privileged users, and from devices dedicated and limited only to authorized persons.
(v) All accounts are protected by strong password policies and multi-factor authentication.
(vi) Access to sensitive data is controlled and limited.
(vii) Data loss prevention software is used to protect sensitive data.
(viii) The procedures for verifying, detecting, analyzing and reporting security incidents are developed and communicated within the organization, mainly through frequent contact with the Compliance Officer.

(x) The procedures for verifying, detecting, analyzing and reporting security incidents are developed and communicated within the organization, mainly through frequent contact with the Compliance Officer.
- Personal and sensitive data is encrypted.
- Folders in the Cloud / Network are encrypted.

Starkdata is committed to the safety and privacy of its customers and their data, and commits to fully following regulations, governance best practices and continuously audit its systems, practices and teams.

Starkdata applies additional appropriate governance and safeguard measures to protect individuals' privacy rights. The Compliance Officer coordinates internally with subject matter experts, and with the Data Protection Officers indicated by its customers.