Data Protection Charter & INPDP–GDPR Compliance Framework

1. Legal Foundations

This Charter reflects HCI's commitment to comply with:

Tunisian Framework (Primary Legal Reference)

- **Organic Law n° 2004-63 of 27 July 2004 on Personal Data Protection**
- **Implementing decrees of Law 2004-63**
- **Decree n° 2018-137 regulating the hosting and processing of health data**
- **INPDP decisions, authorizations, and guidance**

European Framework (Applied When Relevant)

When processing involves EU residents, EU-funded projects, or cross-border IT environments, HCI voluntarily aligns with the GDPR (Regulation (EU) 2016/679), specifically regarding:

- **Transparency**
- **Data minimization**
- **Security and confidentiality**
- **Fair and lawful processing**
- **International transfers**

GDPR applies only in activities involving EU data subjects or EU partners; Tunisian law remains the primary governing framework.

2. Principles of Processing

2.1 Legitimacy & Purpose Specification

HCI collects data strictly for legitimate, explicit purposes, such as:

- **Startup incubation and follow-up**
- **Event and training registration**
- **Talent management**
- **Grant, reporting, and project compliance obligations**
- **Health innovation ecosystem activities**

No processing is performed without legal basis or explicit purpose.

2.2 Consent (Article 12 of Tunisian Law 2004-63)

Where consent is required, HCI ensures it is:

- **Express**
- **Specific**
- **Informed**
- **Freely given**
- **Revocable at any time**

For EU residents, consent follows GDPR standards when applicable.

3. Data Security Measures

In compliance with Article 18 of Law 2004-63, HCI implements:

- **Secure servers and encrypted environments**
- **Authentication, password, and access-control policies**
- **Incident response procedures**
- **Limited access based on role and necessity**
- **Regular assessment of risks and vulnerabilities**
- **Secure disposal or anonymization after retention period**

3.1 Protection of Sensitive/Health Data

Health data requires the highest level of protection.

HCI enforces:

- **INPDP authorization procedures when applicable**
- **Hosting exclusively through providers meeting Decree 2018-137 requirements**
- **Restricted access to authorized personnel only**
- **Prohibition of unapproved external storage or cloud transfers**

For EU projects involving health-related data, HCI aligns with GDPR Article 9 safeguards.

4. Rights of the Data Subject

4.1 Under Tunisian Law (Applicable to All)

- **Right of Access (obtain a copy of your data)**
- **Right of Rectification (correct or update data)**
- **Right of Opposition (object to processing for legitimate reasons)**

4.2 Additional Rights for EU Residents (GDPR Context)

When GDPR applies, individuals may also exercise:

- **Right to Erasure ("Right to Be Forgotten")**
- **Right to Restriction of Processing**
- **Right to Data Portability**
- **Right to Object to Automated Decision-Making**

These rights apply only where HCI processes personal data under EU jurisdictional context.

5. International Transfers

5.1 Strict Tunisian Framework (Default Rule)

HCI does not transfer personal data outside Tunisia unless:

1. **Prior authorization from the INPDP is obtained, and**
2. **The destination country ensures equivalent protection.**

5.2 EU Context (When GDPR Applies)

Cross-border transfers involving EU residents use GDPR mechanisms, such as:

- **Standard Contractual Clauses (SCCs)**
- **Adequacy decisions**
- **Contractual safeguards ensuring equivalent protection**

Unauthorized transfers are strictly prohibited.

6. Retention, Archiving, and Deletion

Data is retained only for the duration necessary for:

- **Program execution**
- **Compliance obligations**
- **Legal and audit requirements**

At the end of the retention period:

- **Data is securely deleted**
- **Or anonymized**
- **Or archived as permitted by law**

Retention schedules are documented and enforced.

7. Accountability & Documentation

HCI maintains:

- **Processing activity logs**

- **INPDP declarations and authorizations**
- **Evidence of consent collection**
- **Security policies and incident reports**
- **Data protection clauses with suppliers and startups**
- **Compliance checklists for EU-related projects**

Audits may be conducted internally or externally.

8. Organizational Responsibilities

8.1 Data Protection Officer (DPO)

The DPO ensures:

- **Compliance with Tunisian and (where applicable) GDPR obligations**
- **Validation of new processing operations**
- **Staff training on data protection**
- **Handling of data subject requests**
- **Liaison with the INPDP**

8.2 Confidentiality Obligations

All staff, mentors, experts, and startups sign confidentiality and data protection commitments.

9. Exercising Your Rights

dpo@healthcareinnovation.tn

10. Review of This Charter

This charter is reviewed annually or whenever Tunisian law, INPDP guidance, or GDPR-relevant requirements evolve.