Digital sovereignty under the magnifier – What does analyzing an IT infrastructure look like?

Take the self-check – How soverign is your infrastructure (excerpt)?

Perform a sovereignty self-check using the questions below. The checklist is a structured, easy-to-understand way to initially assess the maturity level of your infrastructure's digital sovereignty. It helps organizations identify relevant criteria, uncover hidden dependencies, and critically question superficial promises.

1. Technological Independence

Use of Open Source:

□ Are the components of the IT infrastructure open source, and are subjected to agreed standards of the Open Source Community?

Stability of the Open Source Community:

□ Are the open source components used maintained and further developed by a stable and active community?

Avoidance of Black Box Components:

□ Are systems avoided whose functionality or dependencies are not transparent?

Migration to Alternative Components:

□ Are there compatible alternatives for essential software, hardware, or services offering comparable functionality?

Autonomously Controlled Build Pipeline:

□ Are in-house CI/CD or verifiable builds from trusted sources used?

2. Vendor Independence

Avoidance of Vendor Lock-ins:

□ Are proprietary technologies or data formats in use that would significantly hinder a potential switch?

Open Interfaces and APIs:

□ Are open interfaces and exchange formats utilized?

Protection of Critical Systems:

□ Are business-critical components explicitly considered and, if necessary, operable and maintainable independently?

3. Support and Crisis Management

Supports Quality:

□ Is (German-speaking) support available, and is it solution-oriented and effective?

Support Responsiveness:

□ Is the support easily reachable, quick to respond, and flexible?

Implementation of crisis management:

□ Are dedicated emergency plans and contact options for various incidents, such as the failure of individual components, in place?

Crisis Management Execution:

□ Are relevant people familiar with the emergency plans and capable of executing them?

4. Competence and Knowledge within the Organization

Responsible IT Usage:

□ Is the IT infrastructure – including security concepts – transparently structured, independently documented, and feasible for everyone involved?

Operation of the IT Infrastructure:

□ Do employees or service providers possess sufficient technical knowledge to ensure independent and secure operations, where appropriate?

Stack Knowledge:

□ Are the involved parties familiar with the entire platform stack?

Exit Strategy:

□ Is there an action plan, including data migration and documentation, for transition or replacement scenarios?

Digital Sovereignty Strategy:

□ Does a comprehensive strategy exist to strengthen digital sovereignty, integrated into all technological and organisational decisions?

5. Contractual Conditions

Transparency of Contract Details and Changes:

□ Are contract and licensing terms for all components clearly formulated, and are changes communicated in a timely manner?

Legal Certainty in Case of Disputes:

□ Are legal grey areas excluded that could cause issues in the event of a problem?

Controlling:

□ Is there monitoring of cost trend and an action plan for annual price increases exceeding 20 %?

6. Legal Aspects

Jurisdiction::

□ Are the IT components subject exclusively to European and German law?

Disclosure Obligations:

□ Are there third-country regulations that could compel providers to disclose data?

Exit Agreements

□ Are clear exit and handover agreements in place, and are they considered in IT planning and emergency management?

7. Data Sovereignty & Protection

Data Location:

□ Is all data stored exclusively in Germany or within the EU?

Data Protection:

□ Are personal data processed fully compliant with the GDPR?

Access Control:

□ Is it clearly defined and documented who has access, for what purpose, and is this access management built on independent principles?

Data Encryption

□ Are data encrypted both in transmitting and storing using an in-house key (no third-party service)?

Exfiltration Protection:

□ Is it ensured that data cannot be exfiltrated via upstream services (e.g., through licence dependencies requiring constant online validation)?

8. Backup and Archiving:

Regular Backups:

□ Are data backups performed regularly?

Data Security:

□ Are backups stored securely under sovereign access control?

Archiving:

□ Are inactive data securely archived?

Deletion:

□ Are obsolete data properly and verifiably deleted?

9. Monitoring:

System Monitoring:

□ Are systems regularly monitored for changes?

Performance Monitoring:

□ Is system performance continuously tracked?

Security Monitoring:

□ Are systems monitored for security issues?

Sovereignty Check:

□ Is the level of digital sovereignty reviewed regularly?

10. Certification and Standardization

Standards:

□ Are accepted standards applied (e.g., BSI, ISO certification, NIS2, SCS)?

Certifizierung:

□ Is the IT infrastructure certified and regularly updated?

Audits:

□ Are regular audits conducted for security-relevant components and processes?