

Table of Contents

Preface	17
PART I - SOVEREIGNTY IN CONTEXT	23
1 Introduction	25
2 The digital sovereignty model	27
3 Defining digital sovereignty	31
3.1 Definition	31
3.2 Different views	32
3.3 Three dimensions	33
3.3.1 The technological dimension.....	34
3.3.2 The legal dimension.....	34
3.3.3 The political dimension.....	34
3.3.4 All dimensions matter.....	35
3.4 100% Sovereignty is impossible	35
3.5 The cost of sovereignty	37
3.6 Actors and stakeholders	38
3.6.1 Public sector actors.....	38
3.6.2 Private sector actors.....	38
3.6.3 Civil society.....	39
3.6.4 Sectors under pressure.....	39
4 How did we get here?	41
4.1 The rise of U.S. hyperscalers	41
4.1.1 Where the modern cloud came from.....	42
4.1.2 How hyperscalers got here.....	42
4.1.3 What does "Hyperscale" mean.....	43
4.1.4 The economics of scale and lock-in.....	44
4.2 Europe's missed opportunities	44
4.2.1 American hyperscalers in Europe.....	45
4.2.2 Europe didn't produce a hyperscaler.....	46
4.2.3 Europe's different path.....	47

4.3	China's clouds.....	47
4.4	Other regions.....	48
4.5	Snowden's leaks	49
4.6	Safe Harbor	50
4.7	Privacy Shield.....	50
4.8	The EU-US Data Privacy Framework.....	52
4.9	The COVID pandemic	52
5	Sovereign clouds in Europe.....	55
5.1	Globalization in a changing world.....	55
5.2	GAIA-X	56
5.3	National sovereign cloud strategies.....	57
5.3.1	France	57
5.3.2	Germany	57
5.3.3	Smaller member states.....	59
5.4	Sovereignty washing	60
6	Public sector requirements	61
6.1	Democratic accountability	61
6.2	The obligation to keep services running	62
6.3	Protecting privacy as a public duty	62
6.4	Protecting defense secrets	62
6.5	Public procurement	63
PART II - LAWS AND REGULATIONS.....		65
7	Europe	67
7.1	The European Union.....	67
7.2	Privacy: The GDPR	68
7.2.1	GDPR principles	68
7.2.2	Data minimization	68
7.2.3	Purpose limitation	70
7.2.4	Storage limitation	71
7.2.5	The Data Protection Officer	72
7.3	Security: NIS2	72
7.3.1	From NIS to NIS2	72
7.3.2	What NIS2 requires.....	73
7.3.3	NIS2 sectors	74
7.4	The EU Data Act	76

7.5	The EU Data Governance Act	76
7.6	The EU AI Act	77
7.6.1	Risk-based classification	77
7.6.2	Transparency	77
7.6.3	Dependency on foreign foundation models.....	78
7.7	Digital trust: eIDAS 2.0	78
8	The United States of America.....	81
8.1	Introduction	81
8.2	Digital sovereignty laws	82
8.2.1	Privacy	82
8.2.2	Cybersecurity response	83
8.2.3	Artificial intelligence.....	83
8.2.4	Digital identity.....	84
8.2.5	Two different visions of digital regulation	85
8.3	Europe’s exposure to U.S. law	85
8.4	Data espionage.....	86
8.4.1	The U.S. PATRIOT Act	86
8.4.2	FISA 702	86
8.4.3	The CLOUD Act.....	86
8.4.4	Executive Order 12333.....	87
8.5	Availability	87
8.5.1	U.S. sanctions	87
8.5.2	Export controls and technology restrictions	88
8.5.3	Presidential executive orders.....	89
8.6	Vendor lock-in	90
8.6.1	Technical lock-in.....	90
8.6.2	Financial lock-in	91
9	Other countries.....	93
9.1	China	94
9.2	India	94
9.3	Japan.....	94
9.4	South Korea.....	95
9.5	Canada	95
9.6	Brazil.....	96
9.7	Mexico	96
9.8	Australia.....	97
PART III – THE SOVEREIGNTY BUILDING BLOCKS ...		99

10	Hardware and silicon	101
10.1	The chip supply chain	102
10.1.1	The silicon foundation	102
10.1.2	The CHIPS acts	104
10.1.3	GPU scarcity	104
10.1.4	Export controls as a geopolitical tool	106
10.2	Open hardware	106
10.2.1	RISC-V	107
10.2.2	OpenPOWER	108
10.2.3	Sovereignty over speed	109
10.3	Sovereign data centers	109
10.3.1	Edge computing	110
10.3.2	Choosing the right data center architecture	110
10.4	Trusted hardware	111
10.4.1	The Trusted Platform Module	111
10.4.2	Secure enclaves	112
10.4.3	Root of trust	114
10.4.4	Hardware Security Modules	114
11	Networking	117
11.1	Internet traffic	117
11.1.1	Submarine data cables	118
11.1.2	BGP for internet routing	119
11.1.3	DNS as the internet address book	121
11.1.4	Internet Exchange Points	122
11.2	Wide Area Networks and sovereignty	123
11.2.1	SD-WAN	123
11.2.2	European SD-WAN providers	124
11.3	Decentralization	124
11.3.1	Peer-to-peer protocols	124
11.3.2	ActivityPub and the Fediverse	125
11.3.3	Decentralization as a tool	125
12	Compute and storage	127
12.1	Introduction	127
12.2	Portability	128
12.2.1	Cloud-agnostic design	128
12.2.2	Planning for portability	128
12.2.3	Exit strategies and portability	129
12.2.4	Testing the exit plan	130
12.3	Containerization	130
12.3.1	OCI containers	131
12.3.2	Container registries	131
12.3.3	Kubernetes	132

12.3.4	Managed Kubernetes vs. self-hosted	132
12.3.5	Kubernetes distributions and lock-in.....	133
12.4	Infrastructure as Code	133
12.4.1	Terraform and OpenTofu.....	133
12.4.2	Pulumi, Ansible, and other tools.....	134
12.4.3	GitOps.....	134
12.4.4	Avoiding provider-specific IaC	135
12.5	Cloud services and portability	136
12.5.1	S3-compatible object storage	136
12.5.2	Standard SQL interfaces	137
12.5.3	Serverless and portability	137
12.5.4	Message queue abstraction	138
12.6	Resilience architecture	139
12.6.1	The four priorities of resilience.....	139
12.6.2	Air-gapping and network segmentation.....	140
12.6.3	Offline-capable systems.....	141
12.6.4	Multi-cloud architecture	141
12.6.5	Non-cloud fallback	142
13	Identity and access.....	143
13.1	Introduction	143
13.1.1	Identity and Access governance.....	144
13.1.2	The identity provider	145
13.1.3	The Microsoft Entra monoculture.....	146
13.2	Identity architecture	147
13.2.1	Open standards for identity	147
13.2.2	Self-hosted open-source identity providers.....	148
13.2.3	Identity Federation.....	149
13.2.4	Break-glass and emergency access	149
13.3	Privileged access management	150
13.3.1	What is a PAM system	150
13.3.2	Open-source PAM tools.....	151
14	Software	153
14.1	Introduction	153
14.1.1	Defining software sovereignty	154
14.2	Sovereignty and security	155
14.3	What is open-source software?	156
14.3.1	How it started	156
14.4	Open Source as a strategic tool	157
14.4.1	European institutional commitments to OSS.....	158
14.4.2	The EU Tech Sovereignty Package.....	158
14.4.3	Member states and OSS	159
14.5	Linux	159

14.5.1	European Linux distributions.....	161
14.5.2	Distributions for sovereign deployments.....	162
14.6	Open-source licensing models	163
14.6.1	Permissive licenses.....	163
14.6.2	Weak Copyleft licenses	163
14.6.3	Strong Copyleft licenses.....	164
14.6.4	Commercial open-source.....	164
14.6.5	Open-core vs. open-source.....	165
14.7	The software supply chain	166
14.8	Software bill of materials	167
14.8.1	SBOMs and governance	167
14.8.2	SBOMs in CI/CD pipelines.....	167
14.9	Building on upstream or downstream versions.....	168
14.9.1	LTS vs. rolling release.....	169
14.9.2	Forking	170
14.10	Software sovereignty as ongoing practice	171
15	Data.....	173
15.1	Introduction	173
15.2	Defining data sovereignty.....	174
15.2.1	Data sovereignty, residency, and privacy	174
15.3	Data classification	175
15.3.1	Classification frameworks.....	175
15.4	Personal data under GDPR.....	177
15.4.1	Sensitive personal data.....	177
15.4.2	State secrets and classified government information.....	177
15.4.3	Critical operational data	177
15.4.4	Record of Processing Activities.....	178
15.5	Data residency.....	178
15.6	Data encryption	179
15.6.1	Symmetric and asymmetric encryption	179
15.6.2	Post-quantum cryptography	179
15.6.3	Key management.....	180
15.6.4	Harvest now, decrypt later	181
15.7	Self-sovereign identity	182
15.7.1	Decentralized Identifiers	182
15.7.2	Verifiable Credentials.....	183
15.7.3	The EU digital identity wallet	184
15.8	Data spaces	184
15.8.1	What is a data space	184
15.8.2	Catena-X	185
15.8.3	Prometheus-X.....	186

15.8.4	The European Health Data Space	186
15.8.5	Joining an existing data space	186
15.8.6	Building a new data space.....	187
15.9	End-to-end encryption.....	187
15.9.1	How E2EE Works	187
15.9.2	E2EE in Signal	188
15.9.3	E2EE in Matrix	188
15.9.4	E2EE in ProtonMail	188
16	AI	191
16.1	Introduction	191
16.1.1	How AI systems work	192
16.1.2	The AI provider landscape.....	193
16.1.3	AI sovereignty	194
16.1.4	The EU AI Act.....	195
16.2	Open-weight models	196
16.2.1	Open-weight vs. open-source AI	196
16.2.2	The open-weight landscape.....	197
16.2.3	Fine-tuning open-weight models	199
16.3	AI training and inference.....	199
16.3.1	Training.....	199
16.3.2	Inference.....	200
16.3.3	Retrieval-Augmented Generation	201
16.3.4	Federated learning	202
16.4	Transparency, explainability, and accountability..	202
16.4.1	Audit trails for AI-assisted decisions	203
16.4.2	Prohibited AI practices under the EU AI act	204
16.4.3	Algorithmic accountability	204
PART IV	- IMPLEMENTATION.....	207
17	Assessing supplier sovereignty.....	209
17.1	European Cloud Sovereignty Framework	209
17.2	SEAL levels	210
17.3	Sovereignty objectives	211
17.3.1	SOV-1: Strategic sovereignty	212
17.3.2	SOV-2: Legal and jurisdictional sovereignty	213
17.3.3	SOV-3: Data and AI sovereignty	214
17.3.4	SOV-4: Operational sovereignty.....	215
17.3.5	SOV-5: Supply chain sovereignty	216
17.3.6	SOV-6: Technology sovereignty	217
17.3.7	SOV-7: Security and compliance sovereignty.....	218
17.3.8	SOV-8: Environmental sustainability sovereignty	219
18	Building a sovereignty roadmap	221

18.1	Self-assessment	221
18.1.1	What Is a self-assessment?	221
18.1.2	Common findings	222
18.2	Sovereignty roadmap.....	224
18.2.1	Connecting the roadmap to a planning.....	224
18.2.2	How to prioritize	225
18.2.3	Sovereignty guardrails.....	225
18.3	Organizational change	226
18.3.1	The sovereignty function	226
18.3.2	Aligning procurement	226
18.3.3	Building the right skills	227
18.3.4	Overcoming resistance.....	227
18.4	Stakeholder communication	228
18.4.1	Discuss sovereignty with non-technical audiences ...	228
18.4.2	Presenting sovereignty to the board	228
18.4.3	The sovereignty charter	229
19	Afterword – The road ahead	231
19.1	Quantum computing	231
19.2	AI governance at scale	232
19.3	The EU digital identity wallet.....	232
19.4	The breakdown of the global internet.....	233
19.5	Broadening of industrial sovereignty	234
19.6	Conclusion	234
PART V - APPENDICES.....		235
Abbreviations		237
Index		239
End notes		243