

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	32
3.2 Different views	33
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	35
3.3.4 All dimensions matter	35
3.4 100% Sovereignty is impossible	36
3.5 The cost of sovereignty	37
3.6 Actors and stakeholders	38
3.6.1 Public sector actors	39
3.6.2 Private sector actors	39
3.6.3 Civil society	40
3.6.4 Sectors under pressure	40
4 How did we get here?	43
4.1 The rise of U.S. hyperscalers	43
4.1.1 Cloud started with AWS	44
4.1.2 Microsoft and Google enter the cloud market	45
4.1.3 Growing to hyperscale.....	46
4.1.4 The economics of scale and lock-in	46
4.2 Europe's missed opportunities	47

4.2.1	American hyperscalers in Europe	48
4.2.2	Europe didn't produce a hyperscaler.....	49
4.2.3	Europe's different path	50
4.3	China's clouds.....	51
4.4	Other regions.....	51
4.5	Snowden's leaks	52
4.6	Safe Harbor	53
4.7	Privacy Shield	54
4.8	The EU-US Data Privacy Framework.....	55
4.9	The COVID pandemic	56
5	Sovereign clouds in Europe.....	59
5.1	Globalization in a changing world	59
5.2	Gaia-X.....	60
5.3	National sovereign cloud strategies.....	61
5.3.1	France.....	61
5.3.2	Germany	63
5.3.3	Smaller member states.....	65
5.4	Sovereignty washing	67
6	Public sector requirements	69
6.1	Democratic accountability	69
6.2	The obligation to keep services running	70
6.3	Protecting privacy as a public duty	70
6.4	Protecting defense secrets	71
6.5	Public procurement	72
PART II - LAWS AND REGULATIONS.....		73
7	Europe	75
7.1	The European Union.....	76
7.2	Privacy: The GDPR	76
7.2.1	GDPR principles	76
7.2.2	Data minimization.....	77
7.2.3	Purpose limitation	78
7.2.4	Storage limitation	79
7.2.5	The Data Protection Officer	80
7.3	Security: NIS2	81
7.3.1	From NIS to NIS2	81
7.3.2	What NIS2 requires.....	82

7.3.3	NIS2 sectors	82
7.4	The EU Data Act.....	85
7.5	The EU Data Governance Act	85
7.6	The EU AI Act	86
7.6.1	Risk-based classification	86
7.6.2	Transparency	86
7.6.3	Dependency on foreign foundation models.....	87
7.7	Digital trust: eIDAS 2.0	87
8	The United States of America.....	89
8.1	Introduction	90
8.2	Digital sovereignty laws	90
8.2.1	Privacy	90
8.2.2	Cybersecurity response	91
8.2.3	Artificial intelligence.....	92
8.2.4	Digital identity.....	93
8.2.5	Two different visions of digital regulation	93
8.3	Europe’s exposure to U.S. law	94
8.4	Data espionage.....	95
8.4.1	The U.S. PATRIOT Act	95
8.4.2	FISA 702	95
8.4.3	The CLOUD Act.....	95
8.4.4	Executive Order 12333.....	96
8.5	Availability	96
8.5.1	U.S. sanctions	96
8.5.2	Export controls and technology restrictions	97
8.5.3	Presidential executive orders.....	99
8.6	Vendor lock-in	99
8.6.1	Technical lock-in.....	99
8.6.2	Financial lock-in	100
9	Other countries.....	103
9.1	China	104
9.2	India	104
9.3	Japan.....	105
9.4	South Korea.....	105
9.5	Canada	105
9.6	Brazil.....	106
9.7	Mexico.....	106
9.8	Australia.....	107

PART III – THE SOVEREIGNTY BUILDING BLOCKS . 109

10	Hardware and silicon	111
10.1	The chip supply chain	112
10.1.1	The silicon foundation	112
10.1.2	The CHIPS acts	114
10.1.3	GPU scarcity	115
10.1.4	Export controls as a geopolitical tool.....	117
10.2	Open hardware	117
10.2.1	RISC-V	119
10.2.2	OpenPOWER	120
10.2.3	Sovereignty over speed	120
10.3	Sovereign data centers	121
10.3.1	Edge computing	122
10.3.2	Choosing the right data center architecture	123
10.4	Trusted hardware	123
10.4.1	The Trusted Platform Module	124
10.4.2	Secure enclaves	125
10.4.3	Root of trust	127
10.4.4	Hardware Security Modules	127
11	Networking	129
11.1	Internet traffic.....	130
11.1.1	Submarine data cables	130
11.1.2	BGP for internet routing	132
11.1.3	DNS as the internet address book	133
11.1.4	Internet Exchange Points	136
11.2	Wide Area Networks and sovereignty	136
11.2.1	SD-WAN	137
11.2.2	European SD-WAN providers	137
11.3	Decentralization	138
11.3.1	Peer-to-peer protocols	138
11.3.2	ActivityPub and the Fediverse	139
11.3.3	Decentralization as a tool	139
12	Compute and storage.....	141
12.1	Introduction	142
12.2	Portability.....	142
12.2.1	Planning for portability.....	143
12.2.2	Exit strategies and portability	143
12.2.3	Testing the exit plan.....	144
12.3	Containerization	145
12.3.1	OCI containers.....	146
12.3.2	Container registries	147

12.3.3	Kubernetes	147
12.3.4	Kubernetes deployment models	148
12.3.5	Kubernetes distributions and lock-in.....	149
12.4	Infrastructure as Code	150
12.4.1	Terraform and OpenTofu.....	150
12.4.2	Pulumi, Ansible, and other tools.....	150
12.4.3	GitOps.....	151
12.4.4	Avoiding provider-specific IaC	152
12.5	Cloud services and portability	153
12.5.1	S3-compatible object storage	153
12.5.2	Standard SQL interfaces	154
12.5.3	Serverless and portability	155
12.5.4	Multi-cloud architecture	155
12.5.5	Message queue abstraction	156
13	Identity and access.....	157
13.1	Introduction	158
13.1.1	Identity and Access governance.....	158
13.1.2	The identity provider	160
13.1.3	The Microsoft Entra monoculture.....	161
13.2	Identity architecture	162
13.2.1	Open standards for identity.....	162
13.2.2	Self-hosted open-source identity providers.....	163
13.2.3	Identity Federation.....	164
13.2.4	Break-glass and emergency access	165
13.3	Self-sovereign identity	165
13.3.1	Decentralized Identifiers	166
13.3.2	Verifiable Credentials	167
13.4	Privileged access management	168
13.4.1	What is a PAM system	168
13.4.2	Open-source PAM tools.....	170
14	Software	171
14.1	Introduction	172
14.1.1	Defining software sovereignty	172
14.2	Open-source software	174
14.2.1	How it started	174
14.2.2	Open-Source as a strategic tool	175
14.3	European institutional commitments to OSS	176
14.3.1	The EU Tech Sovereignty Package.....	176
14.3.2	Member states and OSS	177
14.4	Linux	178
14.4.1	European Linux distributions	179
14.4.2	Distributions for sovereign deployments	181

14.5	Open-source licensing models	181
14.5.1	Permissive licenses.....	182
14.5.2	Weak Copyleft licenses	182
14.5.3	Strong Copyleft licenses.....	182
14.5.4	Commercial open-source.....	183
14.5.5	Open-core vs. open-source.....	183
14.5.6	Foundation-governed OSS projects.....	184
14.6	Building on upstream or downstream versions.....	185
14.6.1	LTS vs. rolling release.....	186
14.6.2	Forking	187
14.7	The software supply chain	188
14.7.1	Software bill of materials	189
14.7.2	SBOMs in CI/CD pipelines.....	190
15	Data	191
15.1	Introduction	192
15.2	Defining data sovereignty.....	192
15.2.1	Data sovereignty, residency, and privacy	193
15.3	Data classification	194
15.3.1	Classification frameworks	194
15.4	Personal data under GDPR.....	195
15.4.1	Sensitive personal data.....	196
15.4.2	State secrets and classified government information.....	196
15.4.3	Critical operational data	196
15.4.4	Record of Processing Activities.....	197
15.5	Data residency	198
15.6	Data encryption and keys	199
15.6.1	How encryption works	199
15.6.2	Key management	200
15.7	The Quantum challenge	201
15.7.1	Post-quantum cryptography	202
15.7.2	PQE and sovereignty	202
15.7.3	Harvest now, decrypt later	203
15.8	End-to-end encryption	203
15.8.1	How E2EE Works.....	204
15.8.2	E2EE in Signal	204
15.8.3	E2EE in Matrix	205
15.8.4	E2EE in ProtonMail	205
15.8.5	The EU digital identity wallet	206
15.9	Data spaces	206
15.9.1	What is a data space	207
15.9.2	Catena-X	207
15.9.3	Prometheus-X.....	208

15.9.4	The European Health Data Space	208
15.9.5	Joining an existing data space	209
15.9.6	Building a new data space.....	209
16	AI	211
16.1	Introduction	212
16.1.1	How AI systems work	212
16.1.2	The AI provider landscape.....	214
16.1.3	AI sovereignty	215
16.1.4	The EU AI Act.....	216
16.2	Open-weight models	217
16.2.1	Open-weight vs. open-source AI	217
16.2.2	The open-weight landscape.....	218
16.2.3	Fine-tuning open-weight models	220
16.3	AI training and inference.....	220
16.3.1	Training	221
16.3.2	Retrieval-Augmented Generation	222
16.3.3	Federated learning	222
16.3.4	Inference	223
16.3.5	Self-hosting models	224
16.4	Transparency, explainability, and accountability..	224
16.4.1	Audit trails for AI-assisted decisions	225
16.4.2	Prohibited AI practices under the EU AI act	226
16.4.3	Algorithmic accountability	226
PART IV	- IMPLEMENTATION.....	229
17	Assessing supplier sovereignty.....	231
17.1	European Cloud Sovereignty Framework.....	232
17.2	SEAL levels	232
17.3	Sovereignty objectives	233
17.3.1	SOV-1: Strategic sovereignty	234
17.3.2	SOV-2: Legal and jurisdictional sovereignty	236
17.3.3	SOV-3: Data and AI sovereignty	237
17.3.4	SOV-4: Operational sovereignty.....	238
17.3.5	SOV-5: Supply chain sovereignty	239
17.3.6	SOV-6: Technology sovereignty	240
17.3.7	SOV-7: Security and compliance sovereignty.....	241
17.3.8	SOV-8: Environmental sustainability sovereignty	242
18	Building a sovereignty roadmap	245
18.1	Self-assessment	245
18.1.1	What Is a self-assessment?.....	246
18.1.2	Common findings.....	247
18.2	Sovereignty roadmap	249

18.2.1	Connecting the roadmap to a planning.....	249
18.2.2	How to prioritize	250
18.2.3	Sovereignty guardrails.....	251
18.3	Organizational embedding	251
18.3.1	The sovereignty function.....	251
18.3.2	Aligning procurement	252
18.3.3	Building the right skills	252
18.3.4	Overcoming resistance.....	252
18.4	Stakeholder communication	253
18.4.1	Discuss sovereignty with non-technical audiences ...	253
18.4.2	Presenting sovereignty to the board	254
18.4.3	The sovereignty charter	254
19	Afterword – The road ahead	255
19.1	Quantum computing	255
19.2	AI governance at scale	256
19.3	The EU digital identity wallet.....	257
19.4	The breakdown of the global internet.....	257
19.5	Broadening of industrial sovereignty.....	258
19.6	Conclusion	259
PART V - APPENDICES.....		261
Abbreviations		263
Index		265
End notes		269