



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Cybersecurity boundaries for data spaces

Dr Andreas Mitrakas
Head of Unit, ENISA

ENCRYPT conference, Athens

17 | 06 | 2025



UNFETTERED INNOVATION -v- PRECAUTION

Data governance and discovery

Legal basis

- Internal market, article 114 TFEU

Innovation v. Precautionary principle

Risk-based approach

European Commission's Communication on the Precautionary Principle (COM(2000) 1)

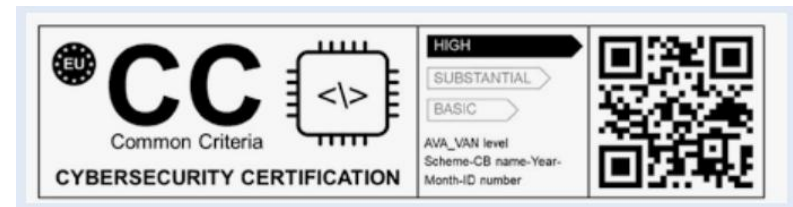
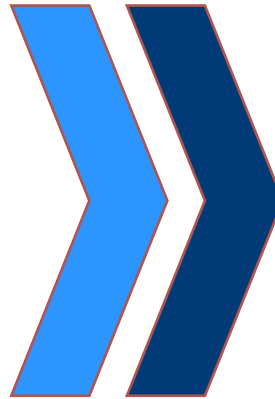
Collinridge dilemma

- Information problem: impact cannot be measured until too late
- Control is challenging ex post facto

Data availability for re-use; data sharing and monetization

Personal data sharing with Intermediaries; data altruism

INFORMATION ASYMMETRY, LEMON LAW



DATA EXCHANGE: REGULATORY PROMPTS

DGA: to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to reuse public data

Data Act: clarifies who can create value from data and under which conditions e.g. IoT

Data Services Act: a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses

DMA: regulate market power-based data

Implementing Act/ Open Data Directive for high value datasets: generally available public data as raw material

Gaia-X: data infrastructure

eIDAS/EUDIW: wallet architecture, interoperability of identity wallets with data wallets

Common Data
Spaces





CLOUD STANDARDS: THE 3 AMIGOS

TS 18037:2025

Business Process
Contextualization

Asset and System
Mapping

CTI

RA

Reference Levels

TS 18026:2024

Security objectives
for cloud services; it
is applicable to
cloud services
providers

TS 18072:2024

Requirements for
CABs assessing
Cloud services; it
may also be used by
NABs

METHODOLOGY FOR
SECTORAL
CYBERSECURITY
ASSESSMENTS

EU Cybersecurity Certification Framework

SEPTEMBER 2021

EUCS – CLOUD
SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme
for cloud services

DECEMBER 2020



SOME PROVISIONS ON PERSONAL DATA

Secure processing environments

Anonymization e.g. differential privacy, synthetic data

Data intermediaries licensing; independence, restrict re-use of data and metadata

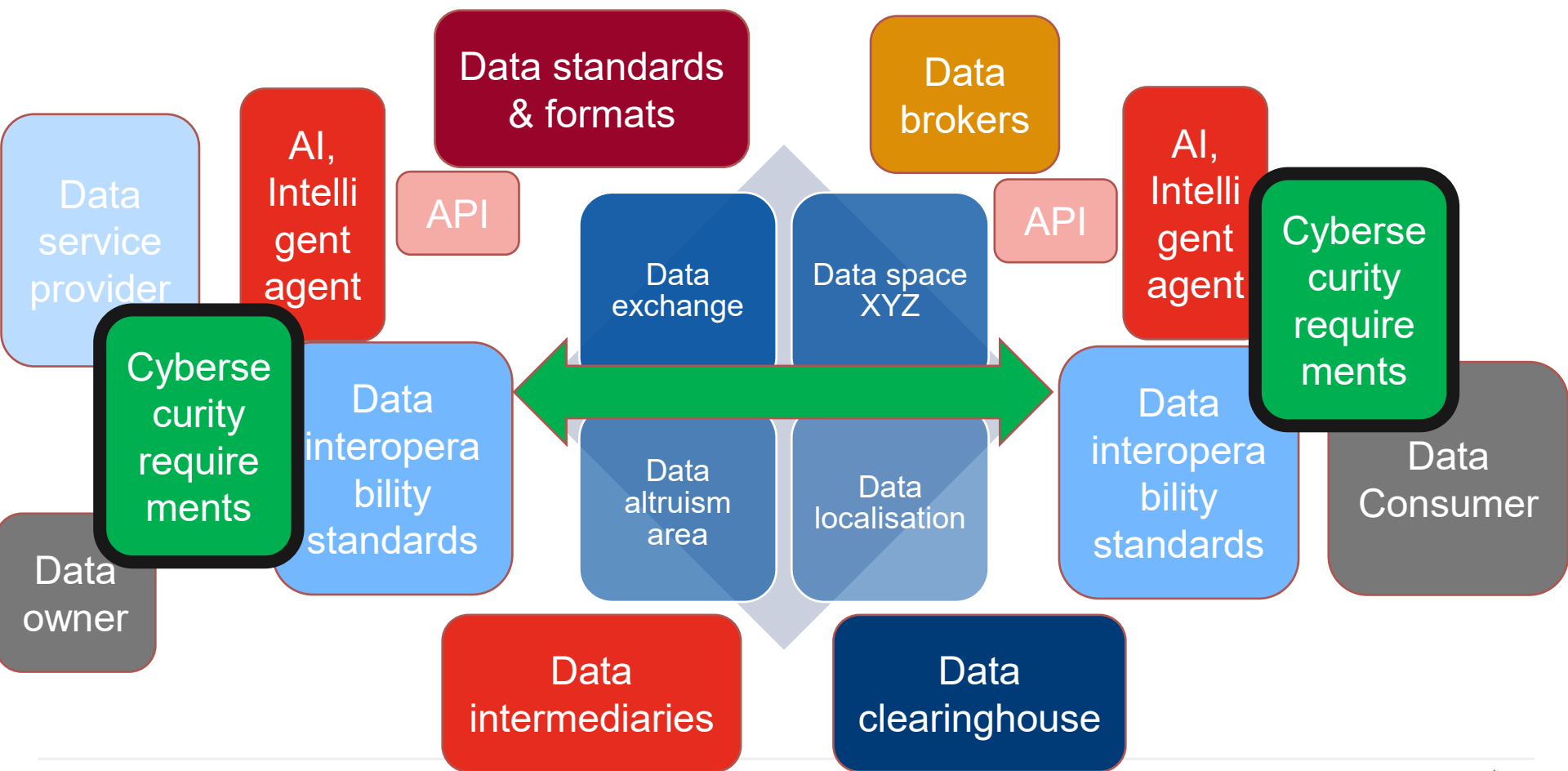
Data marketplaces, consent management platforms e.g. Adtech

Not-for-profit scientific data aggregators may consider a data altruism capacity

Open, assertive international data flows based on EU values; adequacy decision

Conditions to segregate personal from non-personal data

DATA EXCHANGE & CONTROL





SOME QUESTIONS

Are the features of data spaces (DS) and critical sectors (CS) sufficiently clear?

Who cares?

Is there public interest?

Is there relevance between DS and CS?

Are there shared cybersecurity goals between DS & CS?

Are there relevant technical requirements to reuse?

Do current standards make sense for DS? Any gaps?

THANK YOU FOR YOUR ATTENTION



☎ +30 28 14 40 9711

✉ info@enisa.europa.eu

🌐 www.enisa.europa.eu