CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

A Cybersecurity Competence Network with leading research, technology, industrial and public competence

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

How to Organize & Protect 21st Century EU Ecosystems

Update on Legal Aspects of Cybersecurity

Arthur van der Wees LLM

Managing Director Arthur's Legal, the global strategic X-by design firm & knowledge partner

Expert Advisor to the European Commission (IoT, Data, Computing, Spectrum, Cybersecurity, Privacy, AI, Robotics & Accountability)

Expert Advisor to Rijksoverheid (Digital Ecosystems, eIDAS, Dynamic Attributes, Data, Cybersecurity, Privacy & Regulations)

Project Leader to various H2020 IoT, Trust, Security, Privacy, Ethics, Accountability & Liability in IoT Domains

Founding Member Alliance for IoT Innovation (AIOTI) & Chair Policy Working Group

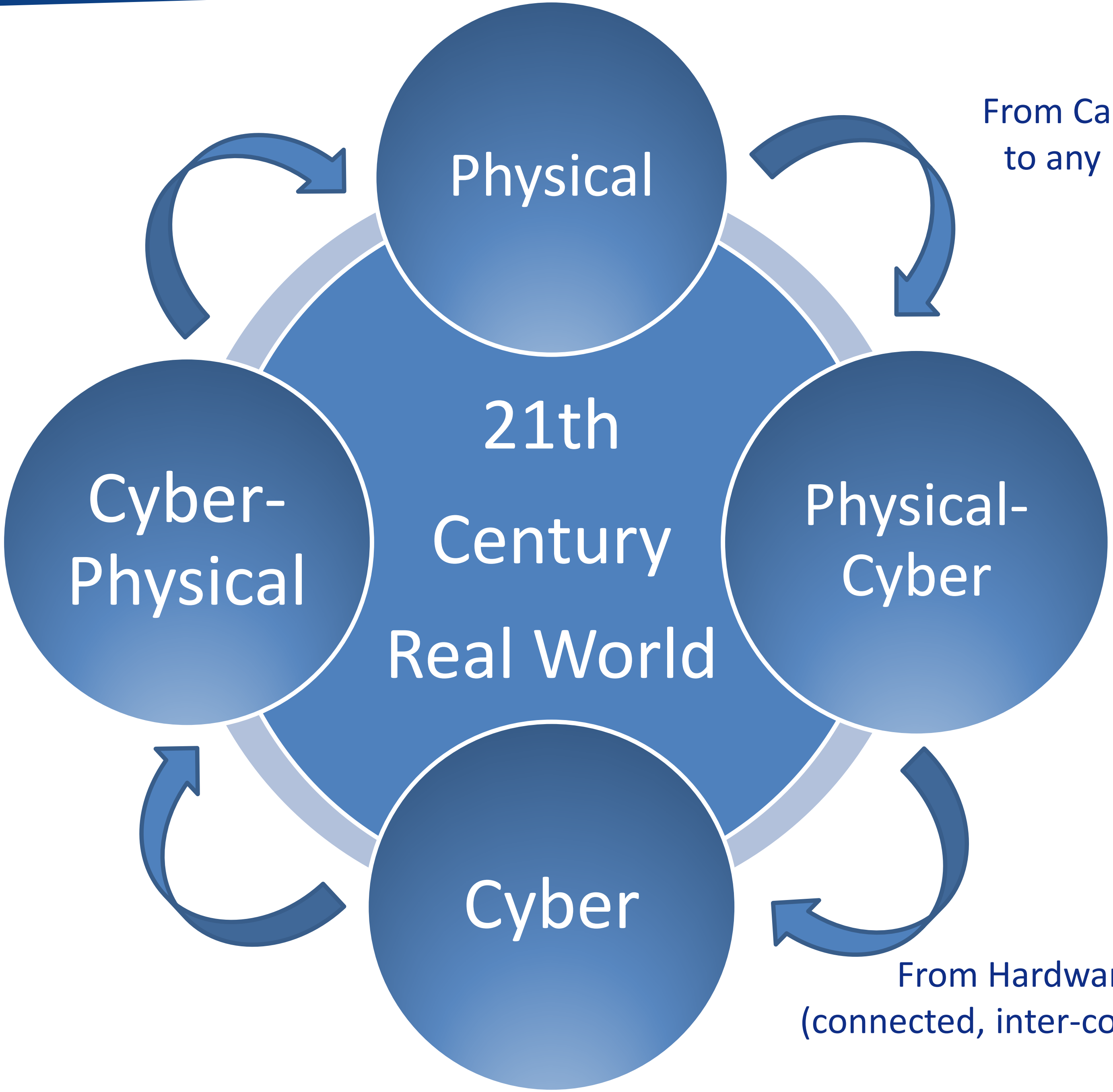
Security in IoT & Privacy in IoT Taskforce Leader AIOTI Standardization Working Group

Specialist Task Force ETSI Leader for Security in IoT & Privacy in IoT (STF 547)

Co-Founder & Director of the Institute for the Future of Living

How to Organize Ourselves? #EU

A. More with Less in the 2020s
B. Europe Fit for the Digital Age
C. What can we do? What should we do?
D. What’s leading by Example?
E. What Next?
F. How to Connect, Collaborate & Co-Create?



From Carbon-based Persons
to any Hardware Gateway

From Hardware Gateway to Cyber
(connected, inter-connected, hyper-connected)

We Are Late

A. More with Less in the 2020s
B. Europe Fit for the Digital Age
C. What can we do? What should we do?
D. What’s leading by Example?
E. What Next?
F. How to Connect, Collaborate & Co-Create?

More Code More Security Less Problems?

SPA: Share Purchase Agreement

Conventional Lawyers Love Complexity & Legacy

It’s just their Business Model

Hackers Love Legacy

Hackers Love Complexity

Convergence & Complexity breads insecurity.
This increased complexity creates new safety, security, privacy, and usability challenges far beyond the difficult challenges individuals face just securing a single device.

Less is More

It’s not too late

For digital devices, systems and services already deployed, **Take Joy** that the millions of insecure digital devices, systems and services are just a small fraction of what the markets and other ecosystems of the Digital Age will resemble in the 2020s.

A. More with Less in the 2020s

B. **Europe Fit for the Digital Age**

C. What can we do? What should we do?

D. What’s leading by Example?

E. What Next?

F. How to Connect, Collaborate & Co-Create?

‘I want Europe to strive for more by grasping the opportunities from the digital age within safe and ethical boundaries.’

Ursula von der Leyen, Candidate President

https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

Digital transformation continues to bring unprecedented changes to every aspect of the economy and society, bringing both new opportunities and new risks.

The main task of the Executive Vice President in this respect will be to ensure that Europe makes the most of the enormous potential of the digital age.

This part of the portfolio contains initiatives aimed at strengthening EU's industry and innovation capacity, as well as its technological leadership and strategic autonomy.

EPRS about Executive VP Margrethe Vestager

http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640171/EPRS_BRI(2019)640171_EN.pdf

Trusted Security is a Need to Have,

not a Nice to Have

Security, Privacy, Compliance & Lack of transparency as Problems?

Seeing the Four Main Blocking Factors for Using Digital Technology as the Main Enablers to Digital Economy & Society:

1. Insufficient knowledge
2. Security
3. (Personal) Data Protection
4. Compliance

Eurostat (EC)

Is Cybersecurity continue to be similar to Patching the Conventional Technology Industry?

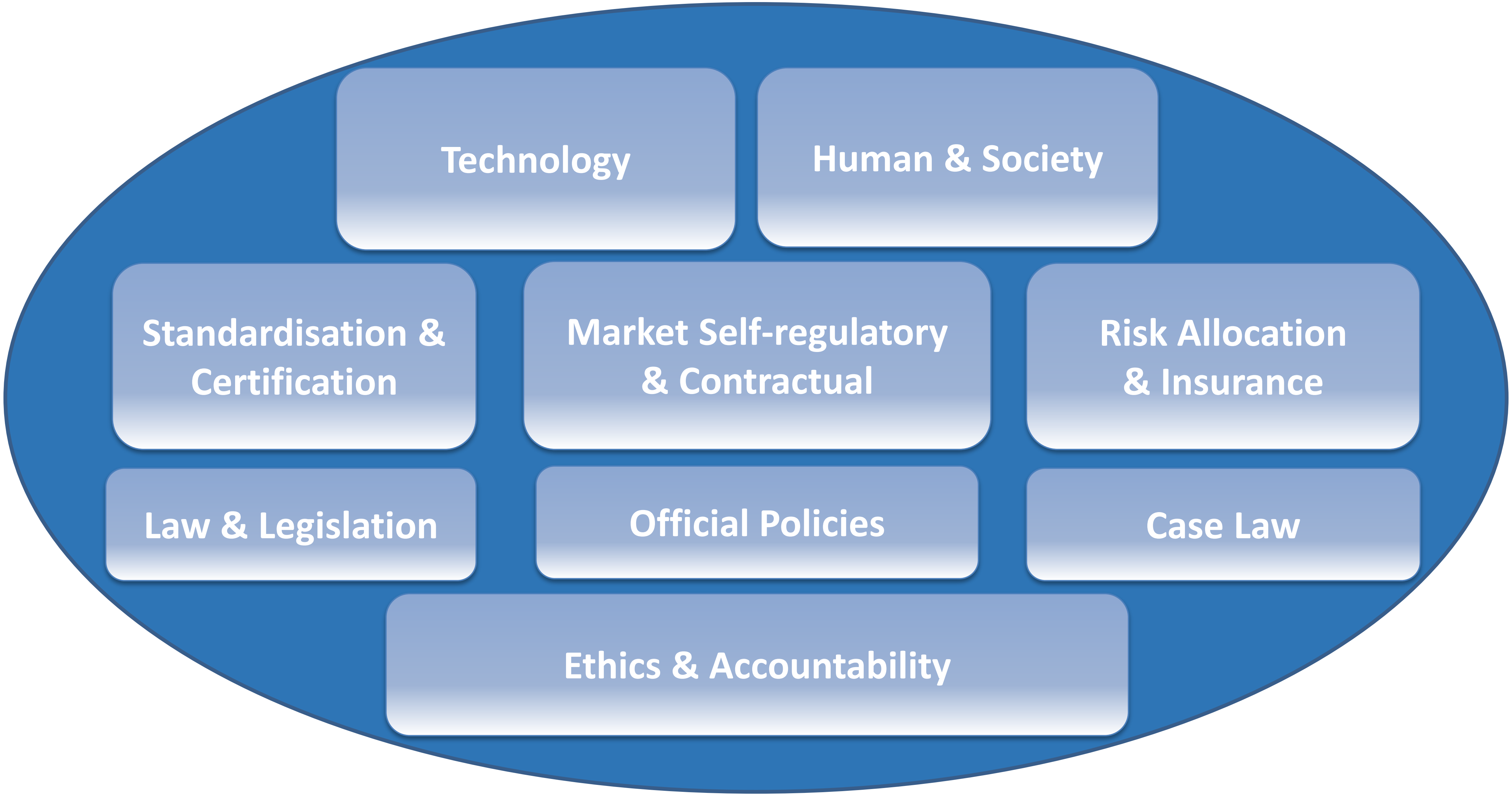
Or will we finally move away from supporting the business model of Build Fast Fix Later?

By Design
By Re-Design
Retrofitting

Pains & Gains

A. More with Less in the 2020s
B. Europe Fit for the Digital Age
C. **What can we do? What should we do?**
D. What’s leading by Example?
E. What Next?
F. How to Connect, Collaborate & Co-Create?

Rule of Law Ecosystem for Transparant, Trust & Trustworthy Frameworks for the Digital Age



Technology

Human & Society

Standardisation & Certification

Market Self-regulatory & Contractual

Risk Allocation & Insurance

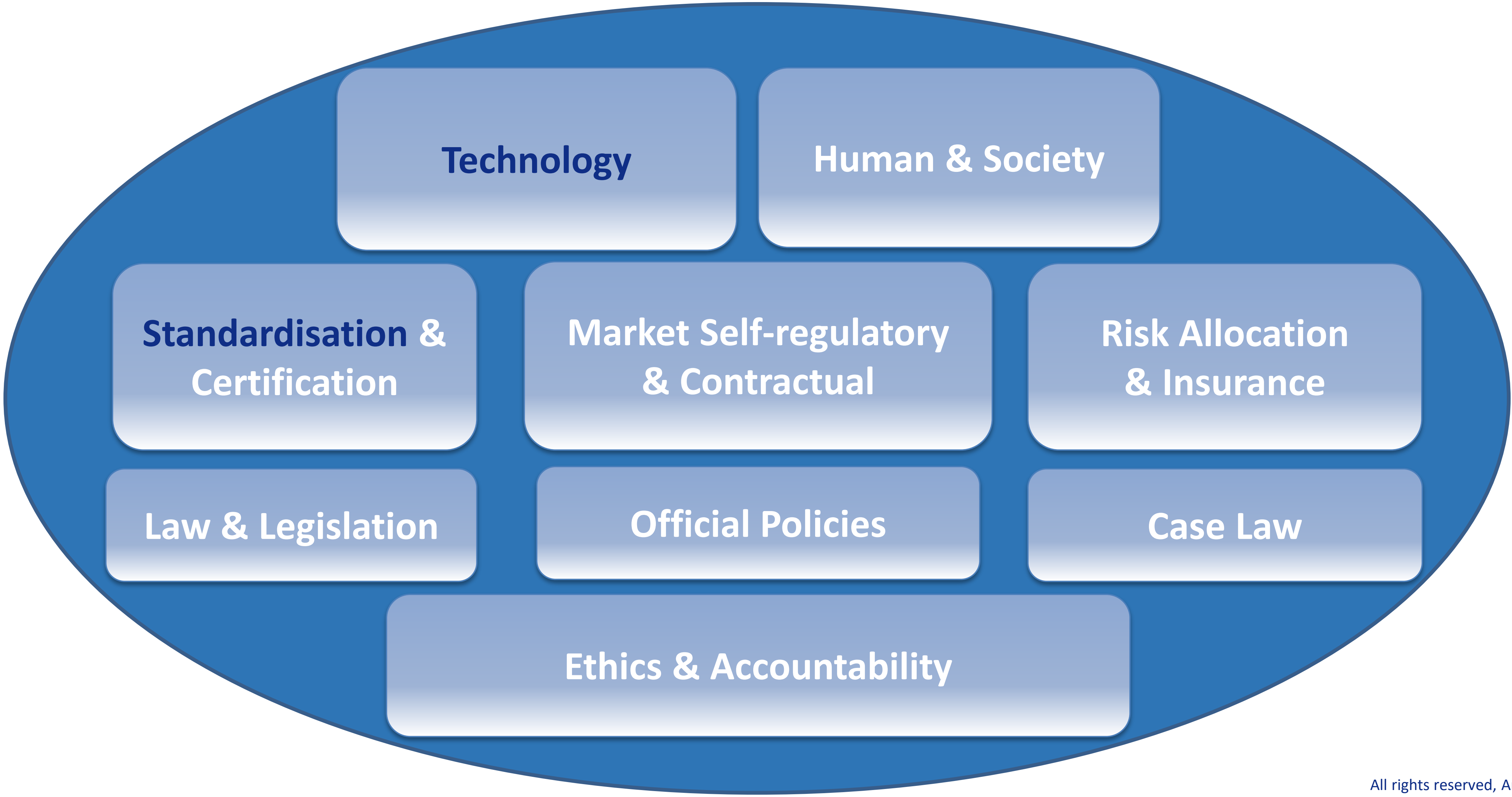
Law & Legislation

Official Policies

Case Law

Ethics & Accountability

Rule of Law Ecosystem for Transparant, Trust & Trustworthy Frameworks for the Digital Age


Technology

Human & Society

Standardisation & Certification

Market Self-regulatory & Contractual

Risk Allocation & Insurance

Law & Legislation

Official Policies

Case Law

Ethics & Accountability

(Personal) Data Protection	Security	Resilience	Risk-Based	Impact-Driven
Privacy	Data Control, Access & Use	Data Management & Analytics	Data Access & National Security	Trust & Trustworthiness
Compliance & Accountability	Sector-Specific Regulation	Liability & Evidence-Based	Interoperability	Identity & Authentication
Data Life Cycle	Legal Life Cycle	Stakeholders Life Cycle	Contextual Life Cycle	Economic Feasibility
Sustainability	Certification & Dynamic Assurance	Code of Engagement	Legislative Instruments	What Else?

ETSI Security Week 2018: Future-Proof IoT Security Standards & Fragmentation as Enablers (Arthur’s Legal Observations)

European Commission

Compared to last years, industry is not making any progress. Zero. We are not seeing any industry-led improvements in the markets regarding security. IoT needs to be made human-centric; one of the key elements is to make it understandable and familiar to users.

GSMA

Mobile operators are in a great position. Baseline on connectivity is there. However, no IoT baseline, yet. More focus on applications and return on investment.

ANEC

Many consumer products do not have any security and privacy features, even though these become more and more cyber-physical. These products however are still on the EU market. There is no appropriate, mandatory legal framework to get and keep these insecure, high-impact/-risk products and services out.

Huawei

Security in IoT is complex but important. Context is everything. By Design and By Default pre-requisites.

Symantec

The attack surface of IoT is even bigger than we currently have. Both-ways & all-the-way, end to end attack scenarios, at least including all technical layers in IoT ecosystems are prerequisites to make security in IoT Future-Proof.

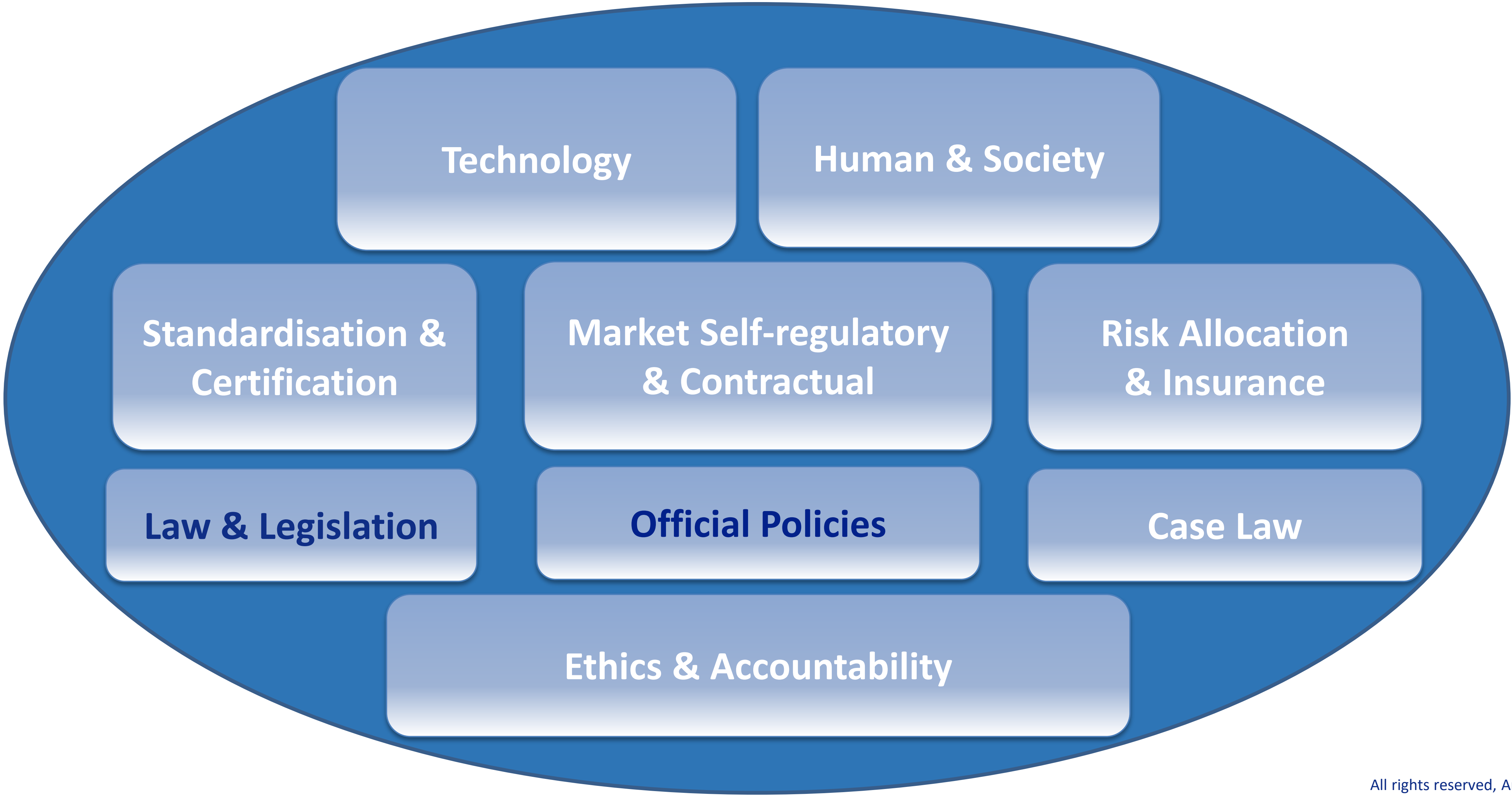
Schneider Electric

Also, in Industry 4.0 and critical infrastructure it is about trustworthiness. A risk-based approach is preferred. Collaboration and education are a need to have.

NXP

Focus on Life Cycle Management of cyber-physical products, systems and services are pre-requisite. From micro-controller all the way to the customer, and its current and future end-users. Collaboration and accountability in security therefore are need to haves.

Rule of Law Ecosystem for Transparant, Trust & Trustworthy Frameworks for the Digital Age



Technology

Human & Society

Standardisation & Certification

Market Self-regulatory & Contractual

Risk Allocation & Insurance

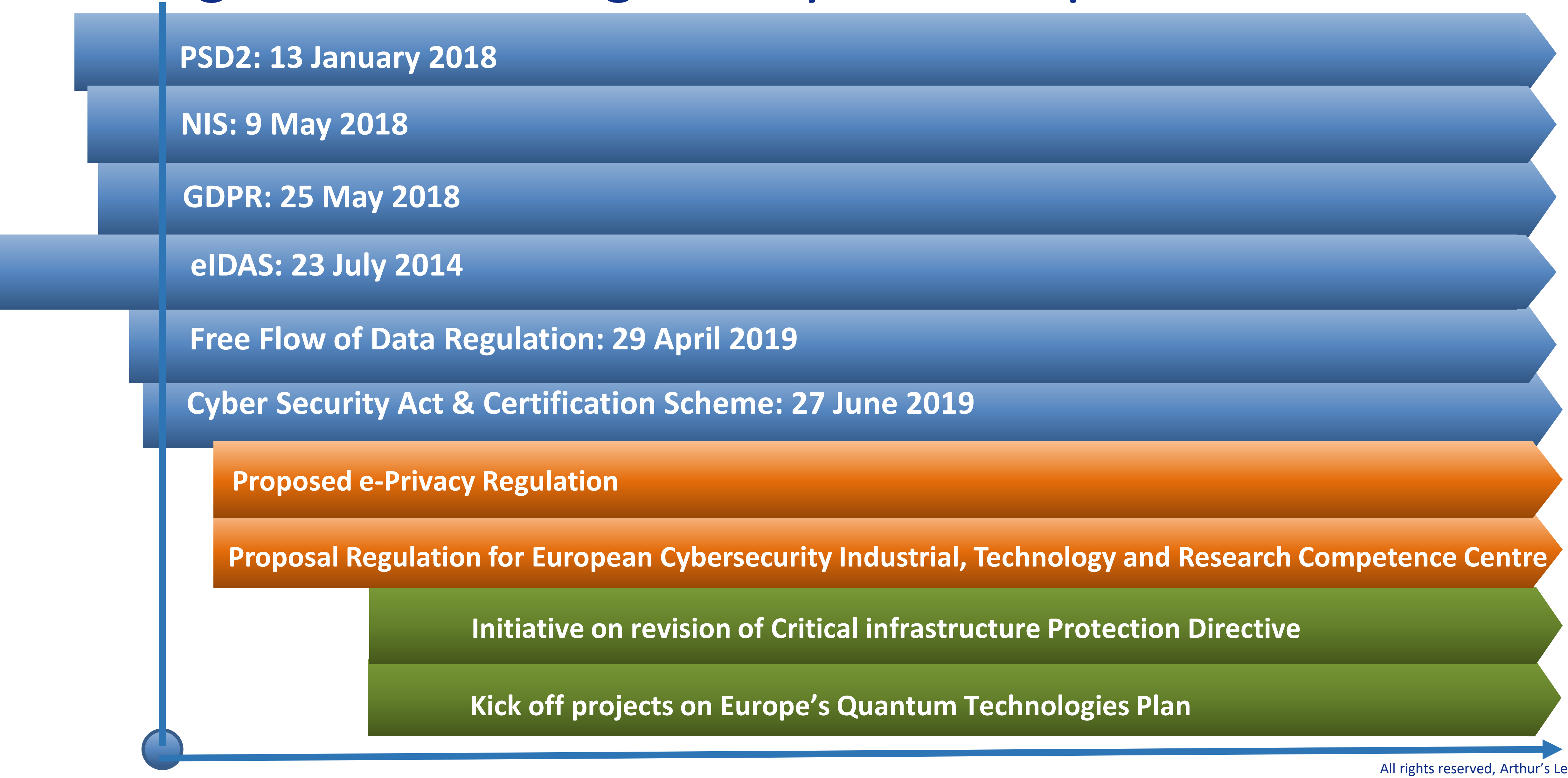
Law & Legislation

Official Policies

Case Law

Ethics & Accountability

Digital & Data Regulatory Landscape (State of Play October 2019)



PSD2: 13 January 2018

NIS: 9 May 2018

GDPR: 25 May 2018

eIDAS: 23 July 2014

Free Flow of Data Regulation: 29 April 2019

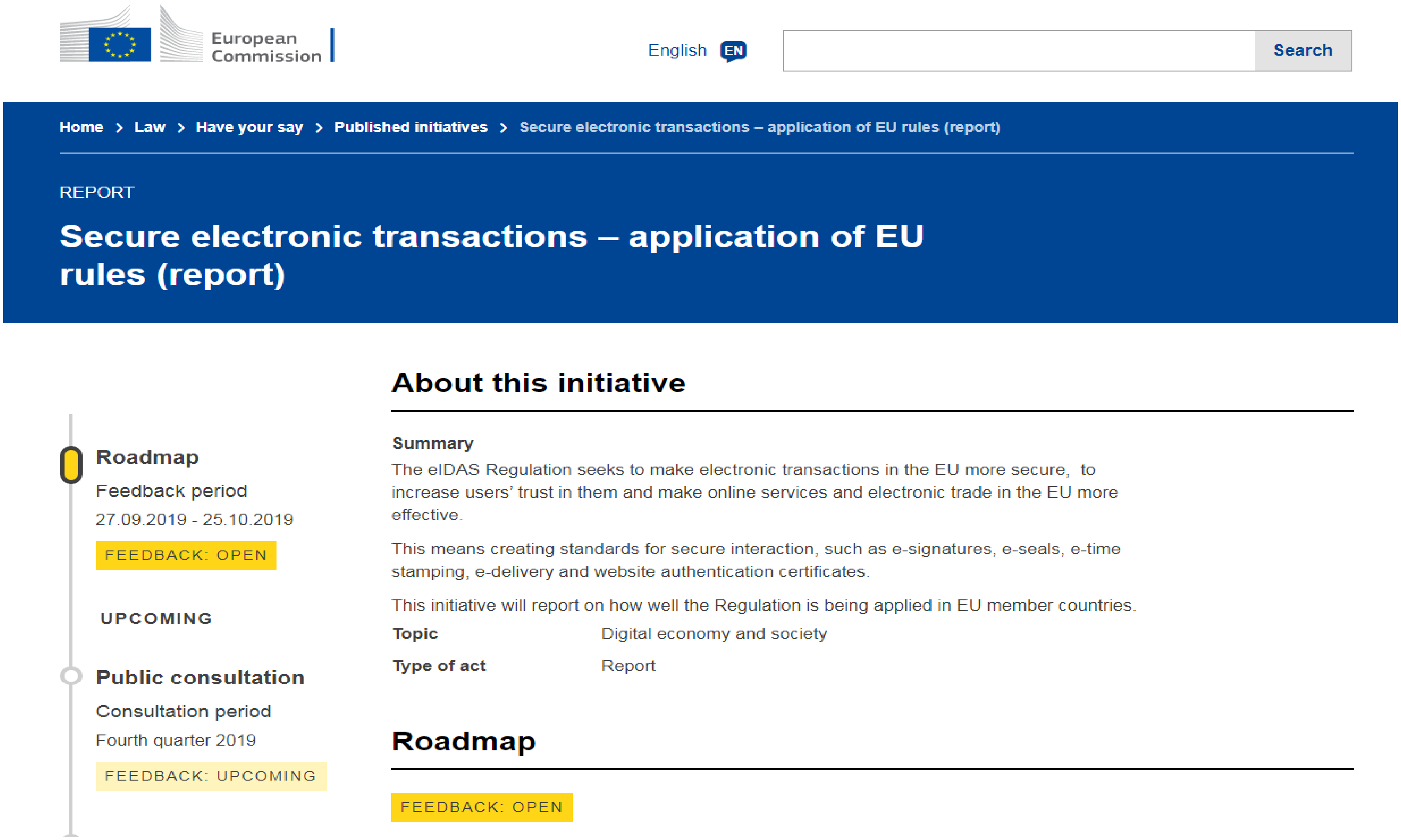
Cyber Security Act & Certification Scheme: 27 June 2019

Proposed e-Privacy Regulation

Proposal Regulation for European Cybersecurity Industrial, Technology and Research Competence Centre

Initiative on revision of Critical infrastructure Protection Directive

Kick off projects on Europe’s Quantum Technologies Plan



Home > Law > Have your say > Published initiatives > Secure electronic transactions – application of EU rules (report)

REPORT

Secure electronic transactions – application of EU rules (report)

Roadmap

Feedback period

27.09.2019 - 25.10.2019

FEEDBACK: OPEN

UPCOMING

Public consultation

Consultation period

Fourth quarter 2019

FEEDBACK: UPCOMING

About this initiative

Summary

The eIDAS Regulation seeks to make electronic transactions in the EU more secure, to increase users' trust in them and make online services and electronic trade in the EU more effective.

This means creating standards for secure interaction, such as e-signatures, e-seals, e-time stamping, e-delivery and website authentication certificates.

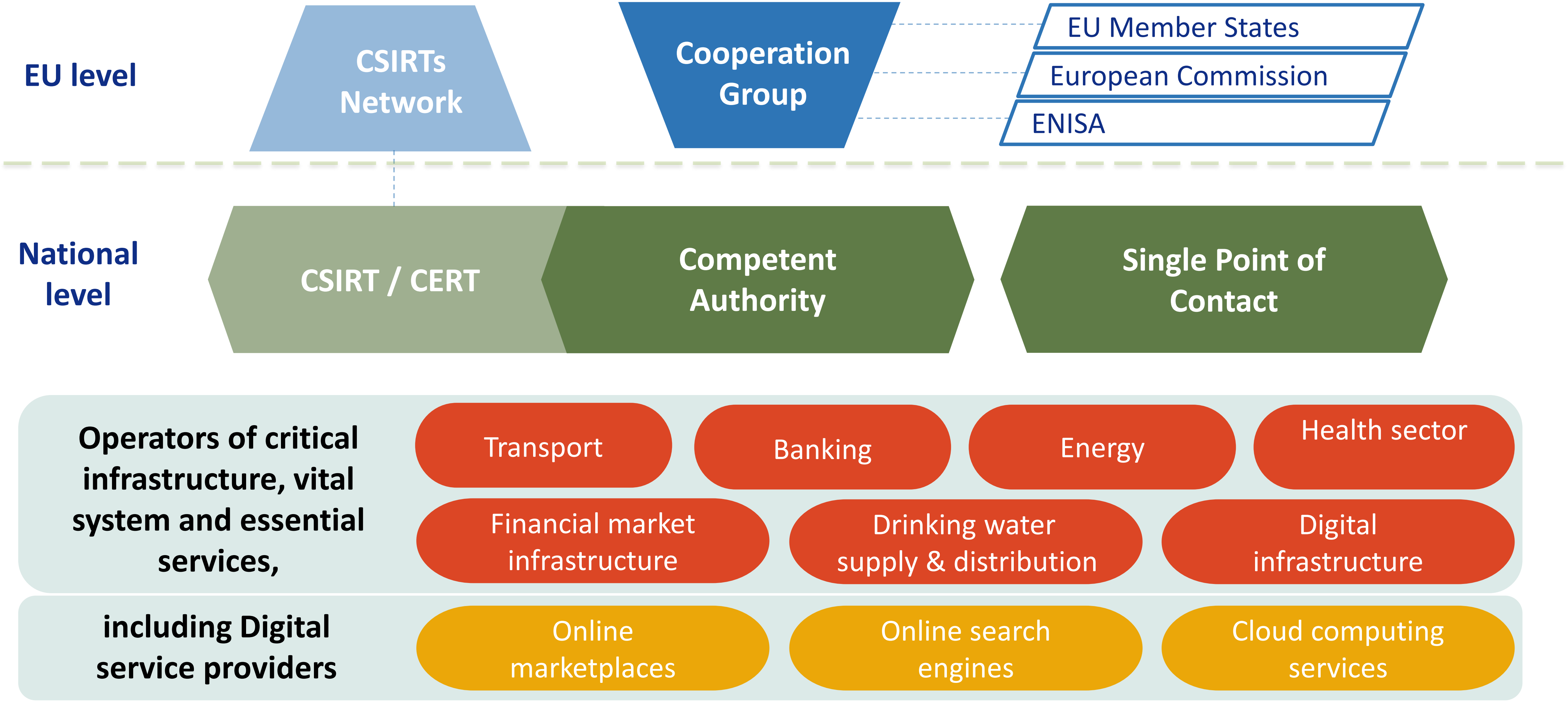
This initiative will report on how well the Regulation is being applied in EU member countries.

Topic	Digital economy and society
Type of act	Report

Roadmap

FEEDBACK: OPEN

NIS Directive Stakeholders



EU level

CSIRTs Network

Cooperation Group

EU Member States

European Commission

ENISA

National level

CSIRT / CERT

Competent Authority

Single Point of Contact

Operators of critical infrastructure, vital system and essential services,

Transport

Banking

Energy

Health sector

Financial market infrastructure

Drinking water supply & distribution

Digital infrastructure

including Digital service providers

Online marketplaces

Online search engines

Cloud computing services

A. More with Less in the 2020s
B. Europe Fit for the Digital Age
C. What can we do? What should we do?
D. **What's leading by Example?**
E. What Next?
F. How to Connect, Collaborate & Co-Create?

From State of Play
to
State of the Art

From Rule-Based to Principle-Based

From Technology-Centric to Technology-Agnostic

From Continual to Continuous

From Compliance to Accountability

Digital Transparency

?

Brief History of the Origin of the GDPR

<1989	No Privacy in CEE
1989	Fall of the Berlin Wall
1995	EU Directive (v1.0)
2011	Start Design Regulation (v1.x)
2018	Regulation (v2.0)

GDPR is Human-Centric

I Am Data

I Have Data. I Control Data.

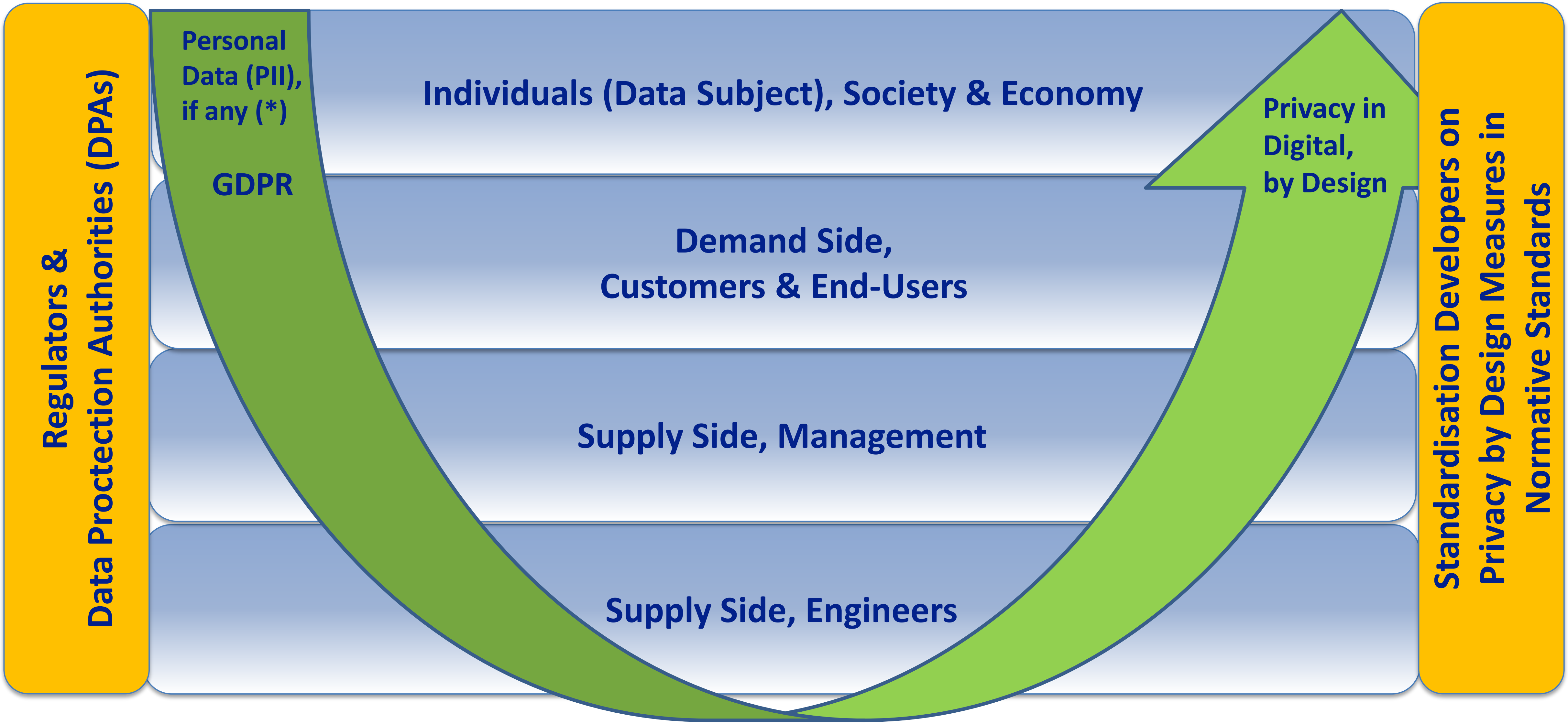
Give me Personalized Services,

Privately, Transparently &

Securely, Please.

A. Technical Measures
B. Organisational Measures
C. Policies & Documentation

Privacy & Trustworthniess by Design Ecosystem



Regulators &
Data Proctection Authorities (DPAs)

Personal Data (PII), if any (*)

GDPR

Individuals (Data Subject), Society & Economy

Demand Side,
Customers & End-Users

Supply Side, Management

Supply Side, Engineers

Privacy in Digital, by Design

Standardisation Developers on
Privacy by Design Measures in
Normative Standards

State of the Art Accountability:

Information Security Standards vs GDPR (25 May 2018)

The GDPR offers an equation for finding the appropriate level of protection, per purpose, per impact assessment, and per economic feasibility. See the Articles 25 & 32 GDPR. We call this the **Continuous Appropriate Dynamic Accountability (CADA) Formula**:

State of the Art Security – Costs – Purposes + Impact

Although the current information security standards aim for ‘**achieving continual improvement**’, the GDPR aims to ensure up-to-date levels of protection by requiring the levels of data protection and security to continuously meet the CADA formula.

A. More with Less in the 2020s
B. Europe Fit for the Digital Age
C. What can we do? What should we do?
D. What’s leading by Example?
E. **What Next?**
F. How to Connect, Collaborate & Co-Create?

GDPR is
Not a Stand-Alone Regulation

Stand-Alone

Connectivity

Inter-Connectivity

Hyper-Connectivity

Forget about Silo-ed & Static Markets

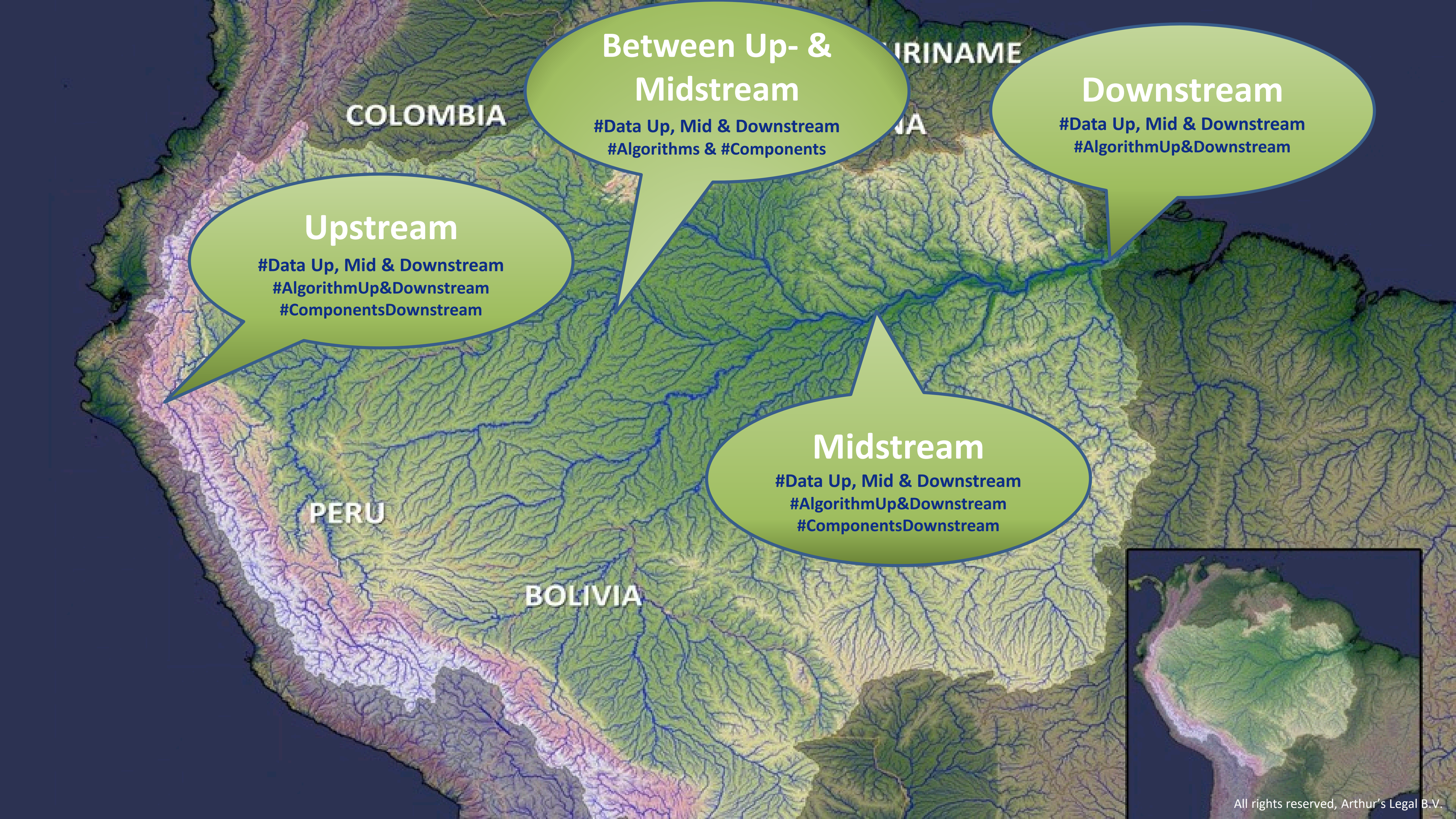
All Market are Converging & Dynamic

The Three T’s

1. Transparency First
2. Trust & Trustworthiness
3. Transformation

Human-Centric Technology, Thriving Ecosystems & Multi-Angled Stakeholders & Influencers

1. The **User** (Convenience-Focused, Cheap, Curious, Creative, Ignorant)
2. **Customers** Who Are Willing To Pay(B2x, x2x)
3. **Suppliers & Value Ecosystem** (Secure In, Secure Inside, Secure Out)
4. Thriving **Ecosystems & Society**
5. **Malicious Actors** (They Are Patient. And They Collaborate! We Do Not)
6. Act First Seek Forgiveness Later **Data Brokers**
7. **Policy** Makers, **Standardisation** Development Orgs & Markets
8. **Authorities** (Who is responsible for what, and are they capable?)
9. **Data Access**: Law Enforcement & Intelligence Services



Upstream

#Data Up, Mid & Downstream
#AlgorithmUp&Downstream
#ComponentsDownstream

Between Up- & Midstream

#Data Up, Mid & Downstream
#Algorithms & #Components

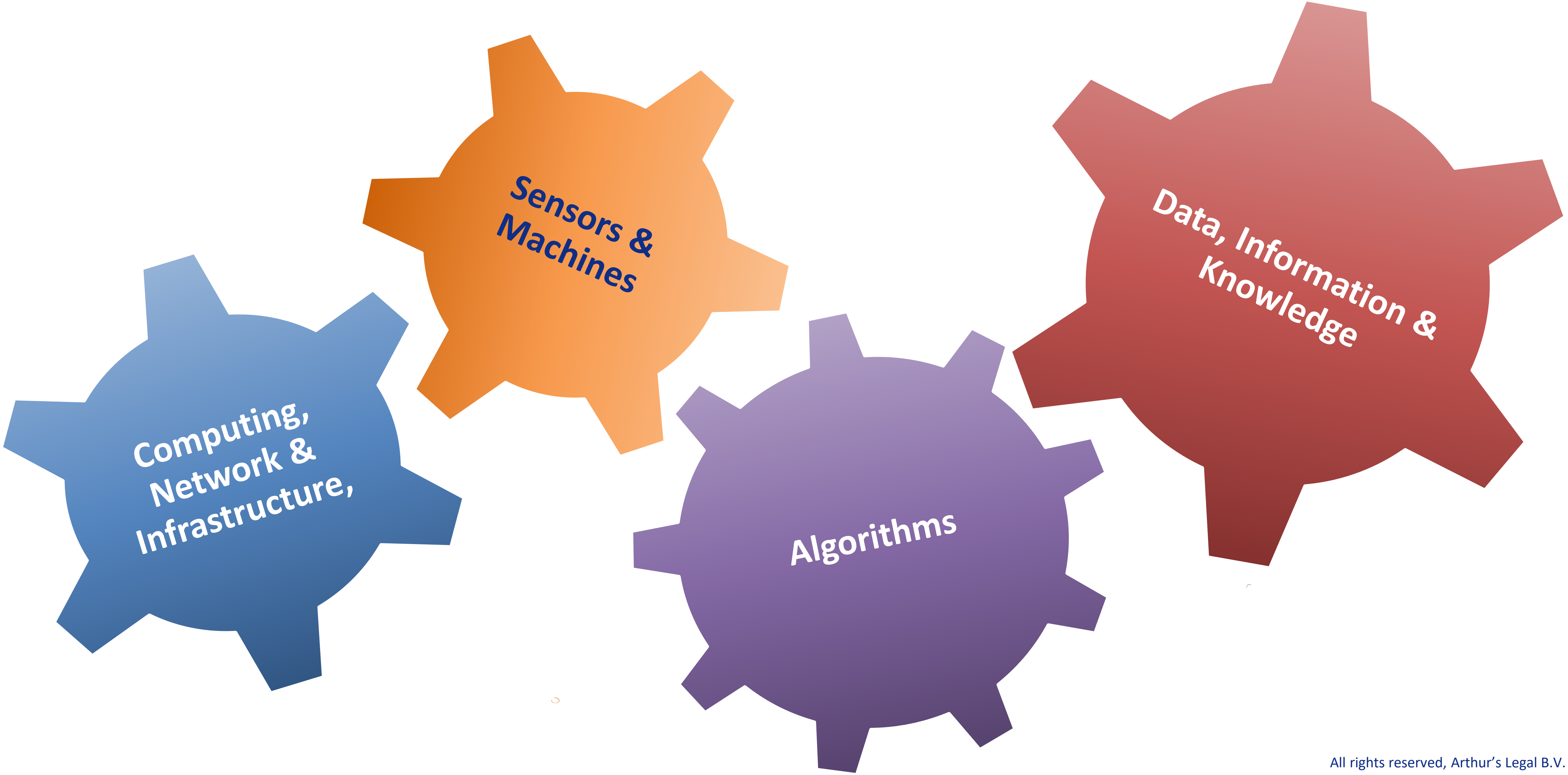
Midstream

#Data Up, Mid & Downstream
#AlgorithmUp&Downstream
#ComponentsDownstream

Downstream

#Data Up, Mid & Downstream
#AlgorithmUp&Downstream

Digital Ecosystems: Interconnected Vessels


Computing, Network & Infrastructure,

Sensors & Machines

Algorithms

Data, Information & Knowledge

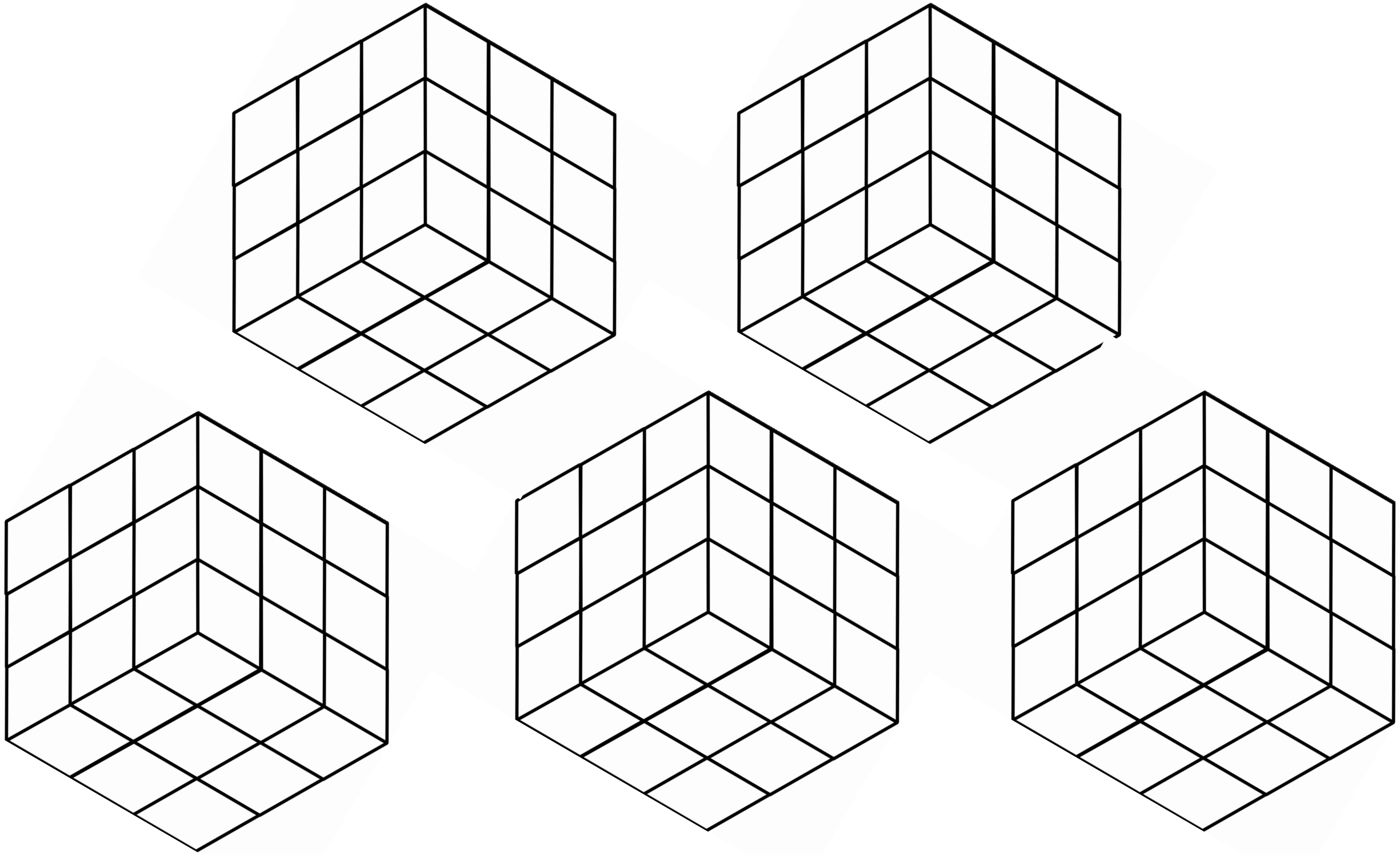
REGULATION IN DIGITAL AGE	NETWORK	SYSTEMS	DATA	APPLICATION	PEOPLE
NIS Directive	✓	✓		Impact-Based?	
Cybersecurity Act	✓	✓	✓	✓	?
Free Flow of Non-Personal Data Regulation		✓	✓	✓	✓
General Data Protection Regulation	✓	✓	✓	✓	✓
Payment Services Directive		✓	✓	✓	✓
Product Liability Directive	?	?	?	?	✓
Radio Equipment Directive	✓	✓	✓	Impact-Based?	
eIDAS Regulation	✓	✓	✓	✓	✓

Ecosystems of Ecosystems in the Digital Age

Connecting Hybercubes to Supercubes

REGULATION IN DIGITAL AGE

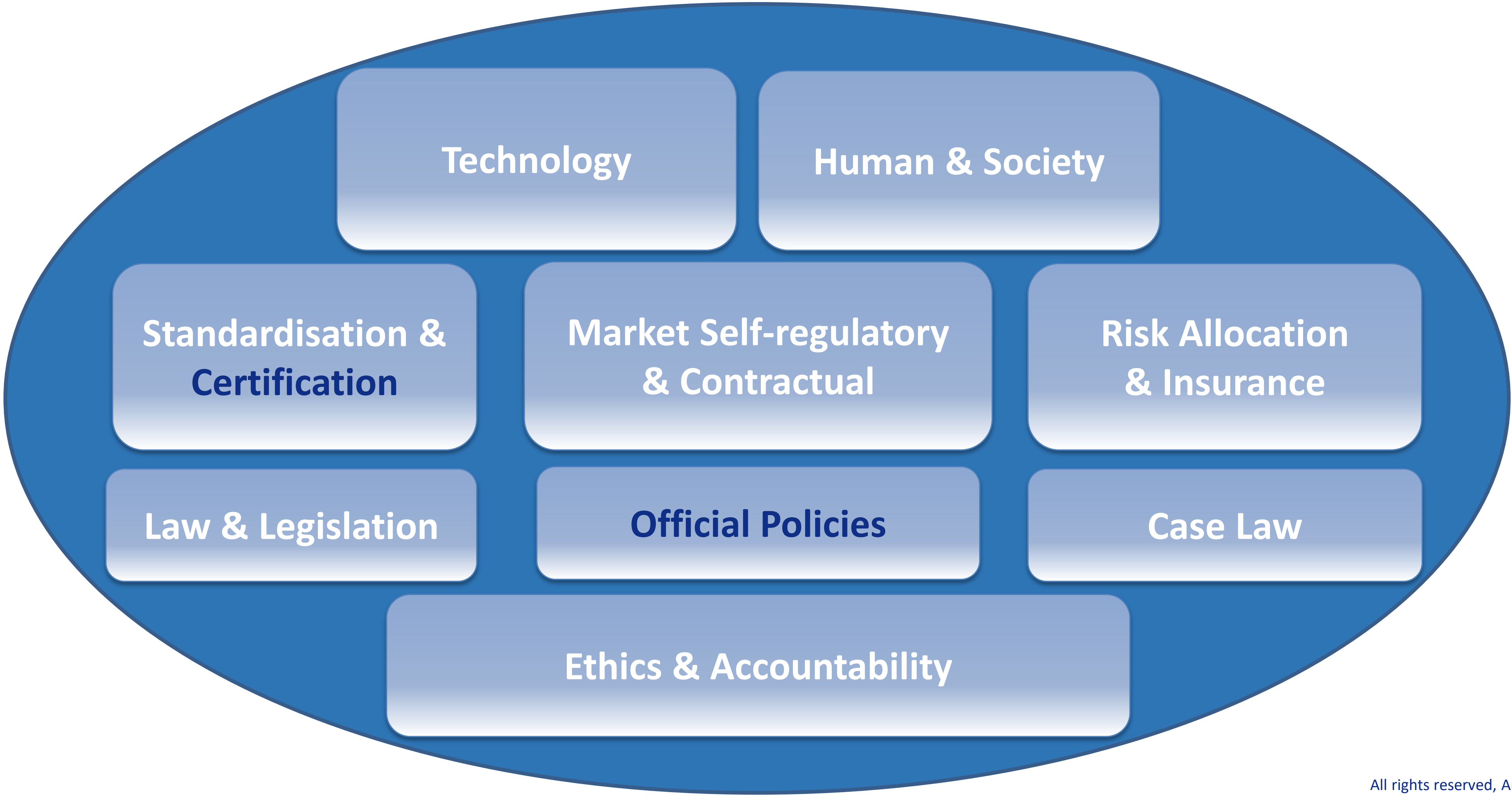
- NIS Directive
- Cybersecurity Act
- Free Flow of Non-Personal Data Regulation
- General Data Protection Regulation
- Payment Services Directive
- Product Liability Directive
- Radio Equipment Directive
- eIDAS Regulation



Frameworks

Please Help Load

Rule of Law Ecosystem for Transparant, Trust & Trustworthy Frameworks for the Digital Age


Technology
Human & Society
Standardisation & Certification
Market Self-regulatory & Contractual
Risk Allocation & Insurance
Law & Legislation
Official Policies
Case Law
Ethics & Accountability

BEREC

EBA

EDA

EDPB

EDPS

ENISA

ETSI, CEN & CENELEC

ISA2

Et cetera

From Static Certification & Dynamic Assurance

How to Validate Continuous SOTA Security, Privacy & Trustworthiness?

And How to Partner Up with Authorities?

Trust, Security, Safety, Privacy & Accountability Principle in the Digital Age

The Principle of No-Surprises

A. More with Less in the 2020s
B. Europe Fit for the Digital Age
C. What can we do? What should we do?
D. What’s leading by Example?
E. What Next?
F. **How to Connect, Collaborate & Co-Create?**

No one has a Monopoly in Cyber

Collaboration therefore is even more Essential.

But not many are succeeding, yet …

This is a Challenging Problem Set

There is No One Solution

There is No One Group with the Answer

There is No One Technical Fixture

This is about Working Together, as Teams

To Achieve Outcomes.

This is a Team Sport

Stop Pointing To The Other One

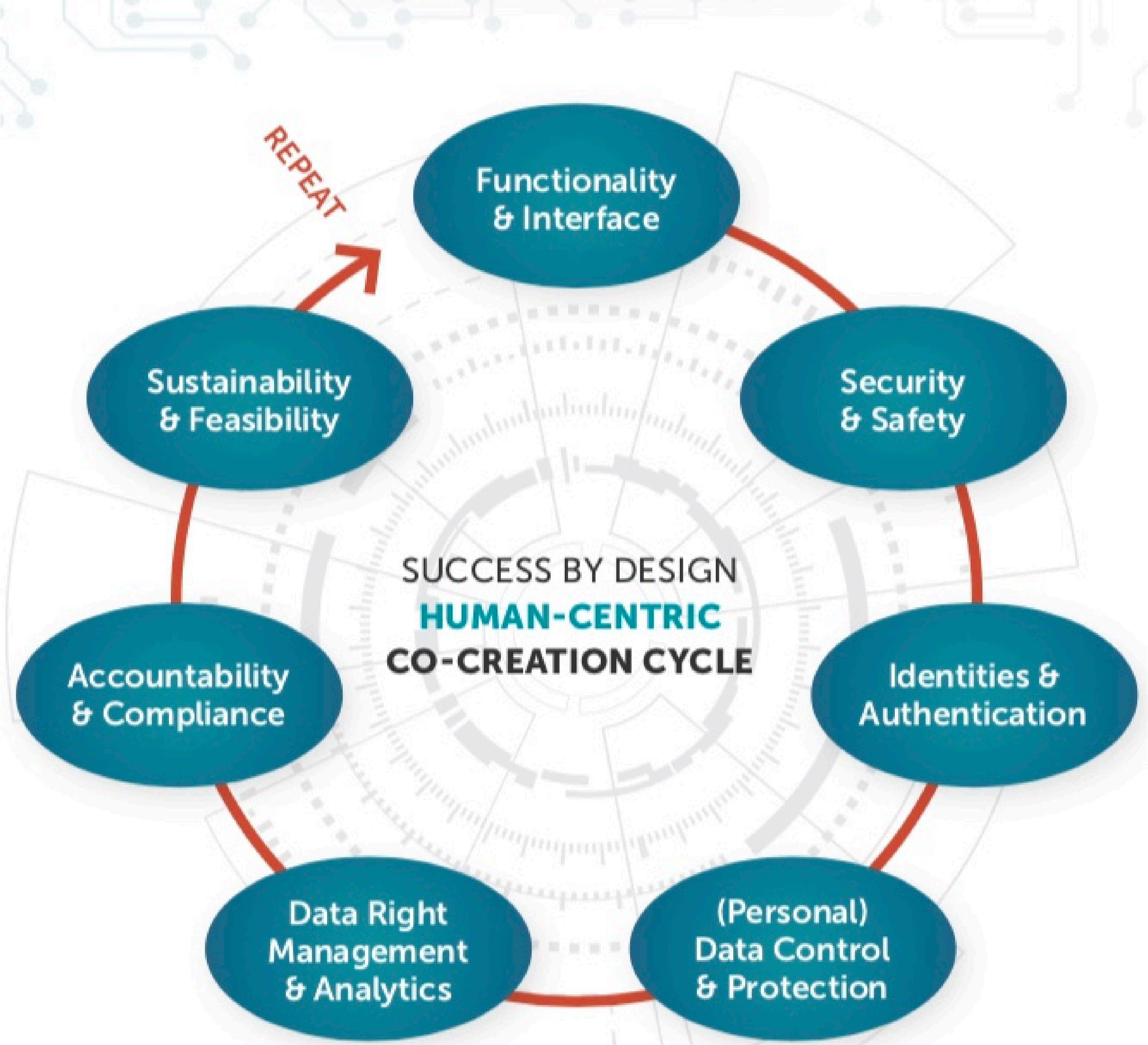
IT'S THEIR RESPONSIBILITY FIRST.
klossner

X By Design

- Security
- Data Protection
- Privacy
- Resilience
- State of the Art
- Transparency
- Trustworthiness
- Engagement
- Accountability
- Competitive Edge

} By Design

Multi-Disciplinary



SUCCESS BY DESIGN
HUMAN-CENTRIC
CO-CREATION CYCLE

Functionality & Interface

Security & Safety

Identities & Authentication

(Personal) Data Control & Protection

Data Right Management & Analytics

Accountability & Compliance

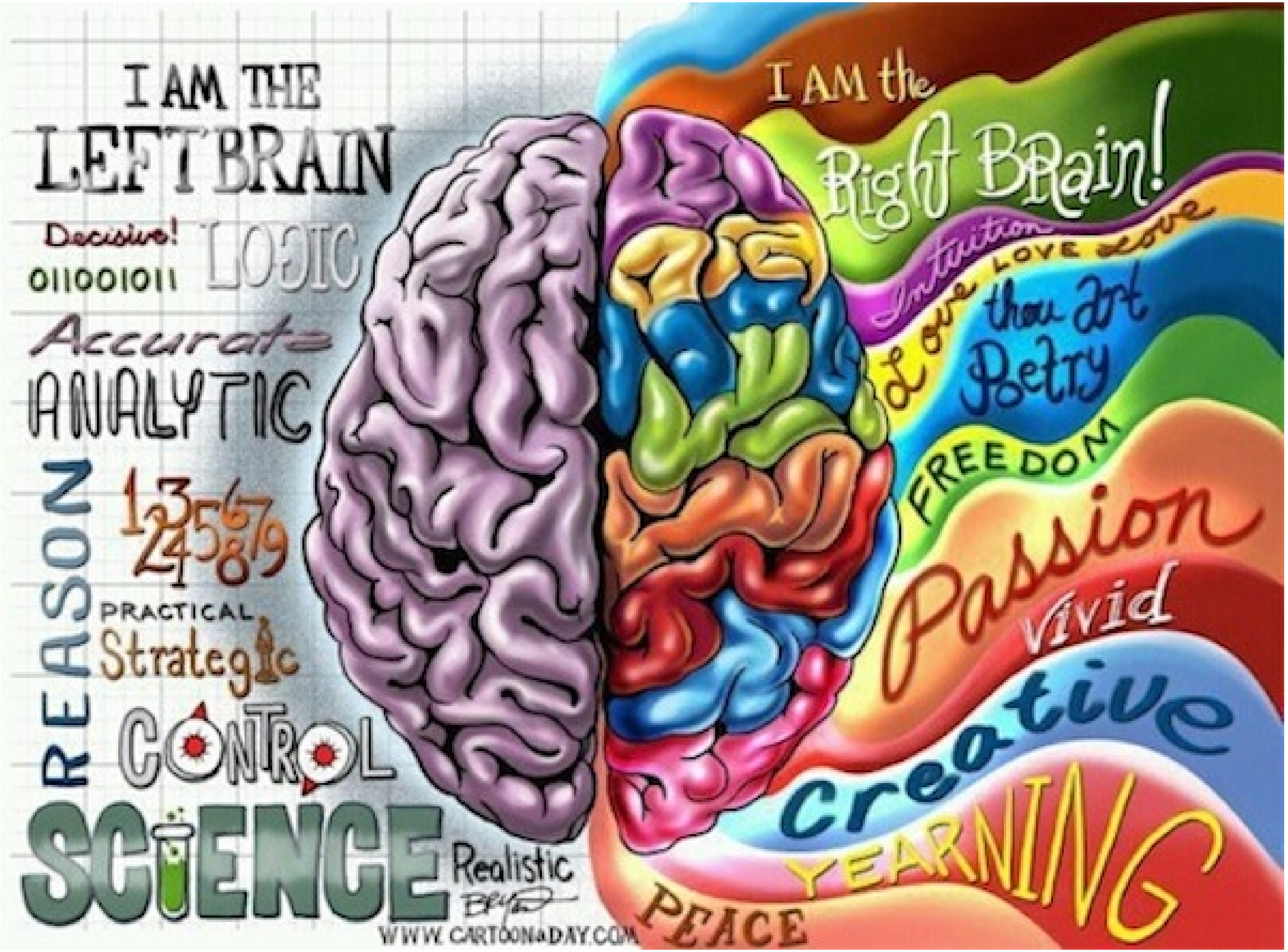
Sustainability & Feasibility

REPEAT

Inter-Disciplinary

Security, Privacy, Transparany & Trustworthiness are Solutions, not Problems

Appropriate Cybersecurity, (Personal) Data Protection & Trustworthiness will enable new markets, promote innovation, and give Customers, Society & Economy confidence to use and enjoy new technologies that improve the quality of life.



Q&A: Anything Goes!

Arthur
vanderwees@arthurslegal.com

Dimitra
stefanatou@arthurslegal.com

Arthurslegal.com
ArthurStrategies.com
@Arthurslegal

ARTHUR'S LEGAL

Challenge the Status Quo

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

in™

www.linkedin.com/in/concordia-h2020