Alliance for Internet of Things Innovation

Security & Privacy in IoT

GDPR in IoT: How To Secure IoT Devices and Related Services to Fulfill Measures Required by the GDPR

Arthur van der Wees

Managing Director Arthur's Legal, the global tech by design law firm & knowledge partner

Expert Advisor to the European Commission (IoT, Data, Cybersecurity, Privacy, AI, Robotics & Accountability)
Project Leader H2020 IoT LSPs & CSAs Activity Group on Trust, Security, Privacy, Accountability & Liability in IoT
Specialist Task Force ETSI (STF 547) Leader for Security in IoT & Privacy in IoT
Founding Member, Alliance for IoT Innovation (AIOTI)
Security in IoT & Privacy in IoT Taskforce Leader AIOTI WG3 (Standardization)
Co-Founder & Co-Chair of the Institute for Future of Living

AIOTI

Smart Everything!

Right?

Welcome to AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

WG 01	IoT European Research Cluster	Smart Living Environment for Ageing Well	Smart Farming and Food Security	Wearables	Smart Cities	Smart Mobility	Smart Water Management	Smart Manufacturing	Smart Energy	Smart Buildings and Architecture
WG 02	Innovation Ecosystems									
WG 03	IoT Standardisation									
WG 04	IoT Policy									
	SME Interests	**WG 05**	**WG 06**	**WG 07**	**WG 08**	**WG 09**	**WG 10**	**WG 11**	**WG 12**	**WG13**

PHILIPS Lighting · vodafone · BOSCH · SIEMENS · SAMSUNG · NOKIA · Schneider Electric · HUAWEI · Telit · infineon · ARTEMIS · ENGINEERING · CATAPULT Digital · Gradiant · life.augmented · IBM · ARTHUR'S LEGAL · CNH INDUSTRIAL · BT · Atos · JOHN DEERE

Global Leading IoT Alliance
acccording to
Forbes

AIOTI

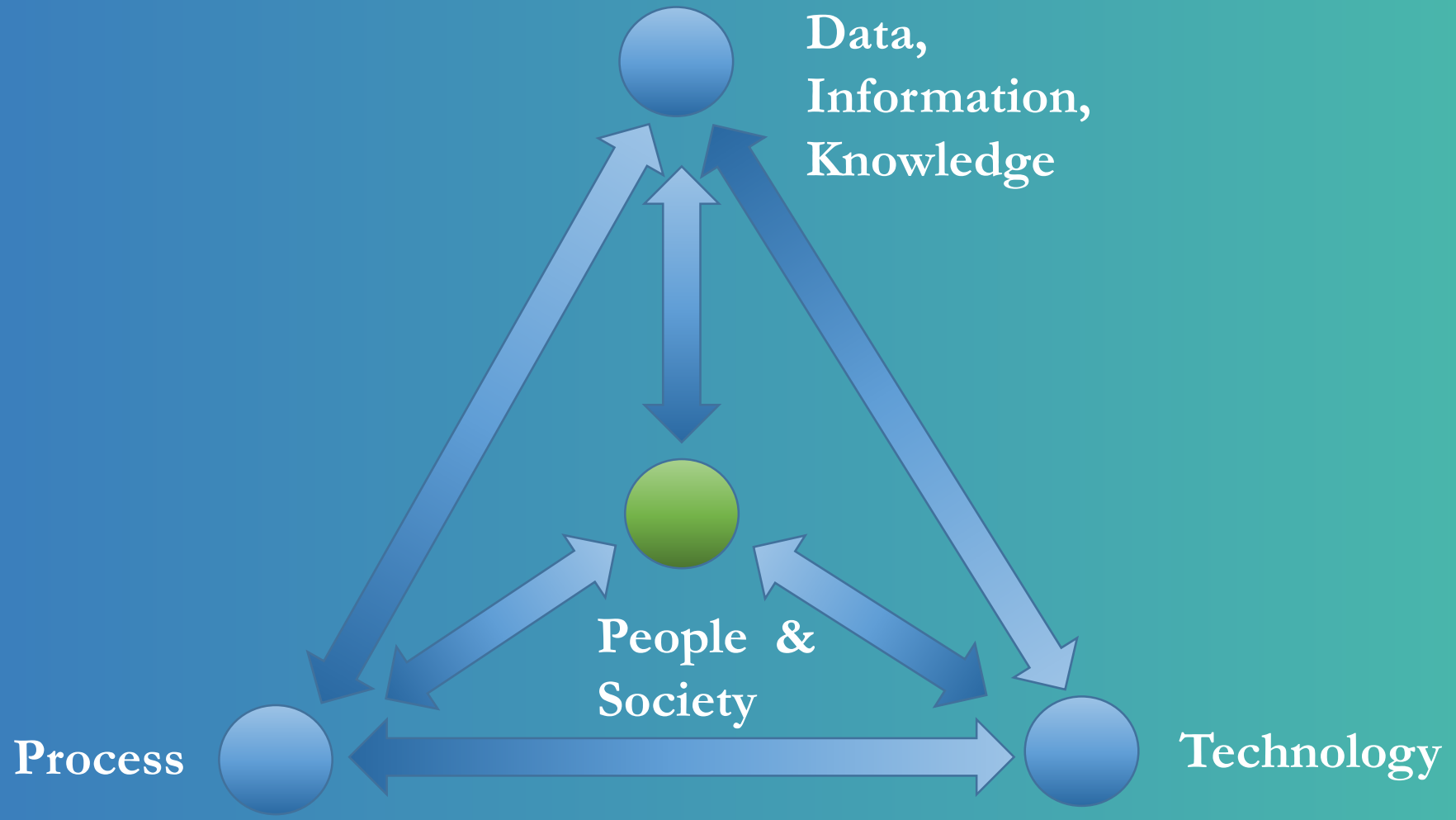
Digital & Data Now Are Highly Regulated Domains

All rights reserved, Arthur's Legal B.V.

AI TI

People, Process, Technology & Data

Human-Centric Organisations & Systems



AIOTI

Demand Side

Customer, User & Society

AIOTI

Risks, Comfort & Trust in Digital Technology

The Four Main Blocking Factors for Using Digital Technology = The Main Enablers to Digital Economy & Society:

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

Eurostat (EC)

Where technology & digital used to be relatively a fairly low regulated horizontal, as it is now considered to be a Need-to-Have, it will become highly regulated in the very near future.

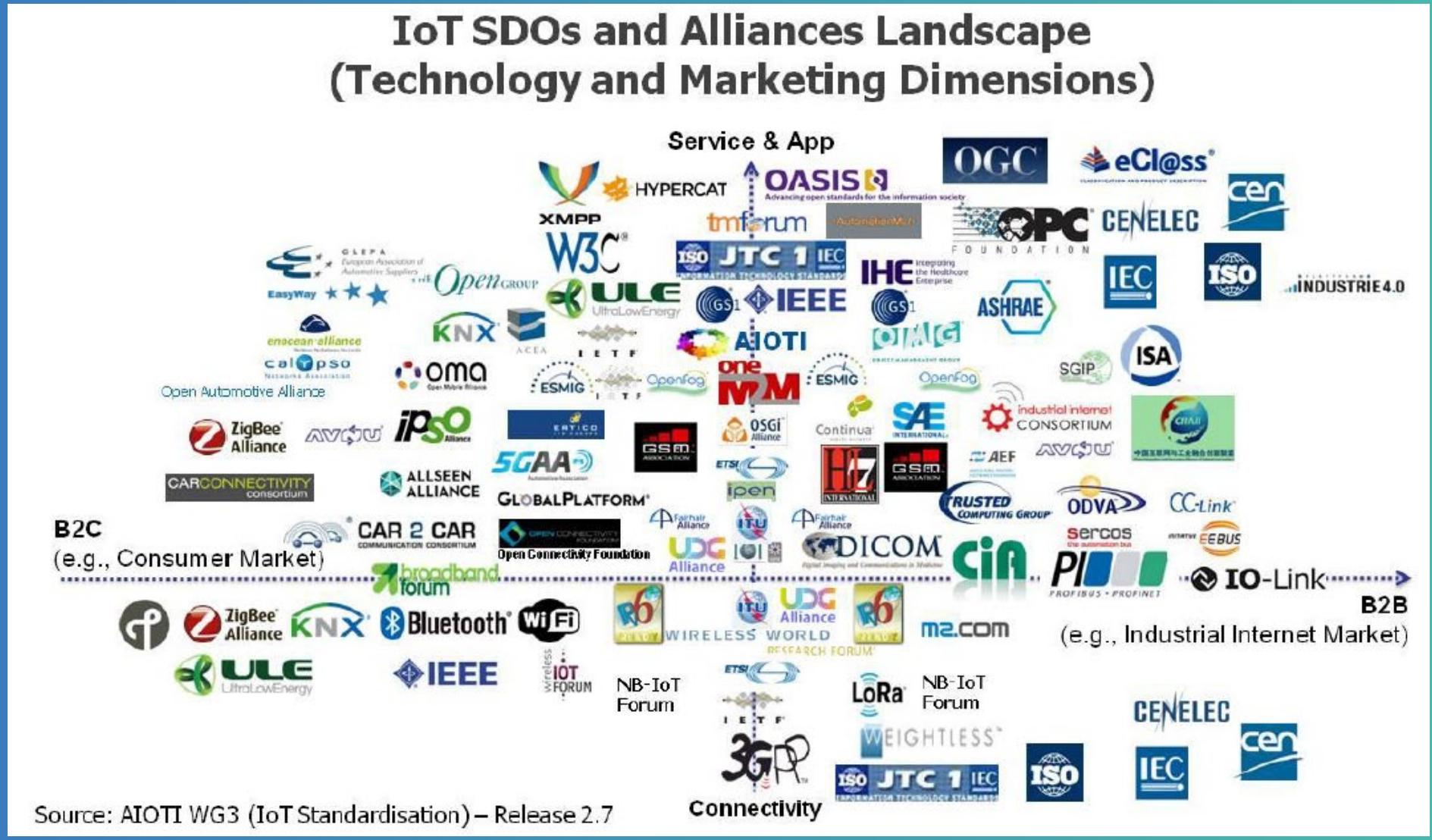
AIOTI

Supply Side:

Industry, Integrator, Vendor, Service Provider

AI TI

Fragmentation



AIOTI

AIOTI

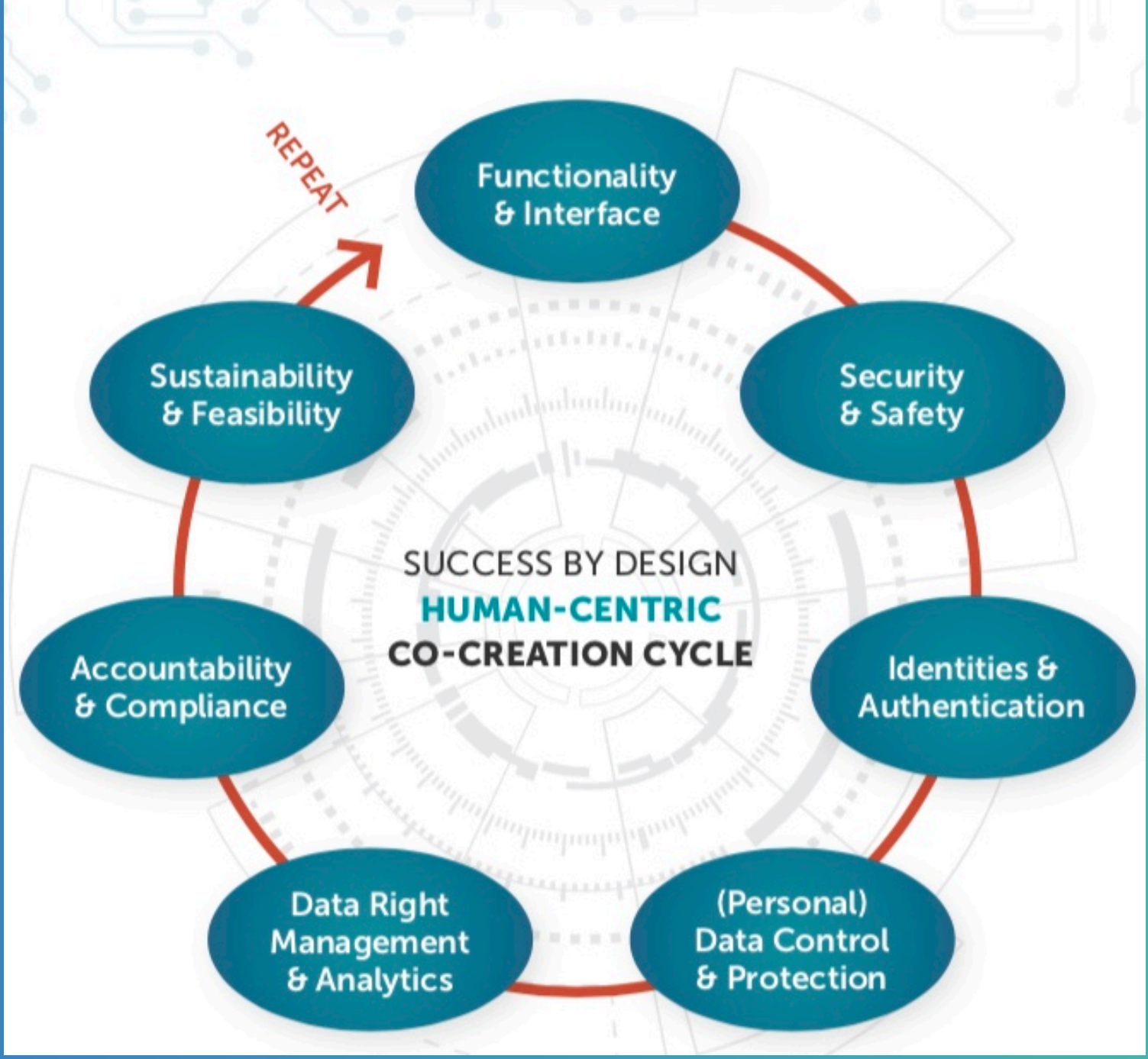
First Half Year 2018:
Security & Privacy in IoT Webinars

GDPR-Centric

A. GDPR: Processing, Protection, Security & Strategies
B. X-by-Design: Upstream & Downstream Resilience
C. State of the Art Privacy Principles & Requirements
D. Consent Management & Engagement in IoT
E. Compliance, Accountability, Assurance & Penalties
F. IoT Ecosystems, Pre-Procurement & Collaboration
G. Data Subject Rights & Data Management in IoT

GDPR Is Not A Stand-Alone Regulation

Multi-Disciplinary



Inter-Disciplinary

AI TI

All rights reserved, Arthur's Legal B.V.

Cybersecurity Act (draft)

Security Objectives (Article 45)

1. Confidentiality, integrity, avaliability and privacy of services, functions, data
2. Ensure authorised access & use of services, functions and data
3. Identification of dependencies and vulnerabilities
4. No vulnerabilities present in ICT products, processes and services
5. Proves to deal with newly discovered vulnerabilities
6. Security by default
7. Up to date software
8. No risk to ecosystem

AI TI

From State of Play to State of the Art

AITI

From Rule-Based to Principle-Based

AI TI

From Continual to Continuous

From Technology-Centric to Technology-Agnostic

AI TI

From Compliance to Accountability

AI TI

Digital Transparency

AI TI

Trust & Trustworthiness

AI TI

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

The Principle of No-Surprises

AIOTI

X By Design

- No Surprises
- Data Protection
- Security
- State of the Art
- Resilience
- Chaos Engineering
- Transparency
- Trust
- Accountability
- Competitive Edge

By Design

AI TI

State of the Art (SOTA)

General State of The Art Layered Plotting Methodology

1. User, Human & Society
2. Data
3. Identity & Authentication
4. Service
5. Software/Application
6. Hardware
7. Infrastructure/Network

AI TI

State of the Art (SOTA) Privacy & Security

Overview of 57 Security in IoT Principles (From 2016 & 2017 EC/AIOTI Reports Only)

1. USER/HUMAN FACTOR
Human-centric approach
Privacy by design
Privacy by default
Decoupling multiple identities
Identity protection by design
Metrics
Independent privacy and security audits
Transparency of data processing
Transparency of privacy policy
Transparent roles
Indication of purpose
Single point of contact
Consent
Non-discriminatory practices
Manufacturer-implemented parametrisation
Accountability

2. DATA
Data segmentation and classification
Privacy by design
'As-if' by design
Data minimisation
De-identification
Data control
Data access
Data ownership
Data management
Data isolation
Security of personal data
Encryption by default
Encryption at the application layer
Standardisation
Accountability
Risk impact assessment by design

3. SERVICES
Life time protection
End of support

4. SOFTWARE/APPLICATION
Security by default
Secure updates
Frequency of updates
Accountability & Liability
Third-party libraries
Information exchange

5. HARDWARE
High-level baseline
Separate safety and security
Security rationale
Security evaluation
Security levels
Sustainability
Assurance
Certification
Trusted IoT label
Defined functions
Secure interface points

6. AUTHENTICATION
Authentication of identities among themselves

7. INFRASTRUCTURE/NETWORK
Harmonised industry approach
Reduce impact of national regulations
Interoperability
Taxonomy
Continuous monitoring

ARTHUR'S LEGAL

UK Department for Digital, Culture, Media &Sport

Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security

A. **Dynamic; Principle-Based; State of the Art; Pro-Active**
B. **Principles in 4 Layers & 3 Dimensions**
C. **The 'As-If' By Design Principle**
D. **Risk Impact Assessment by Design**
E. **Life Cycles (Full Life Time; End to End Security)**
F. **Accountability by Design**

IoT Device Life Cycle	Data Life Cycle	Stakeholders Life Cycle	Contextual Life Cycle	Data Life Cycle

AIOTI

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 **Appropriate Dynamic Accountability (ADA) 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 ADA formula.

AI TI

Dynamic Certification & Assurance

How to Validate Continuous SOTA Security, Privacy & Trustworthiness?

And How to Partner Up with Authorities?

AI TI

New Series IoT Security, Privacy & Trust Webinars
IoT Verticals meet Horizontals

Themes Webinars, Open Attendance: AIOTI, CREATE-IoT, IoT LSPs, H2020 IoT Security Cluster, ETSI STF547, EGNSS and: You!?

The IoT Application-Centric Series

A. Personal Wearables (H2x): Health, Living, Public Space
B. Moving Sensors (M2x): Farm2Food, Mobility, Cities
C. Long Term Fixed IoT Applications (M2x): Industry 4.0, Cities, Water management, Energy, Construction, Living

Subscribe at www.arthurslegal.com/iot

AIOTI

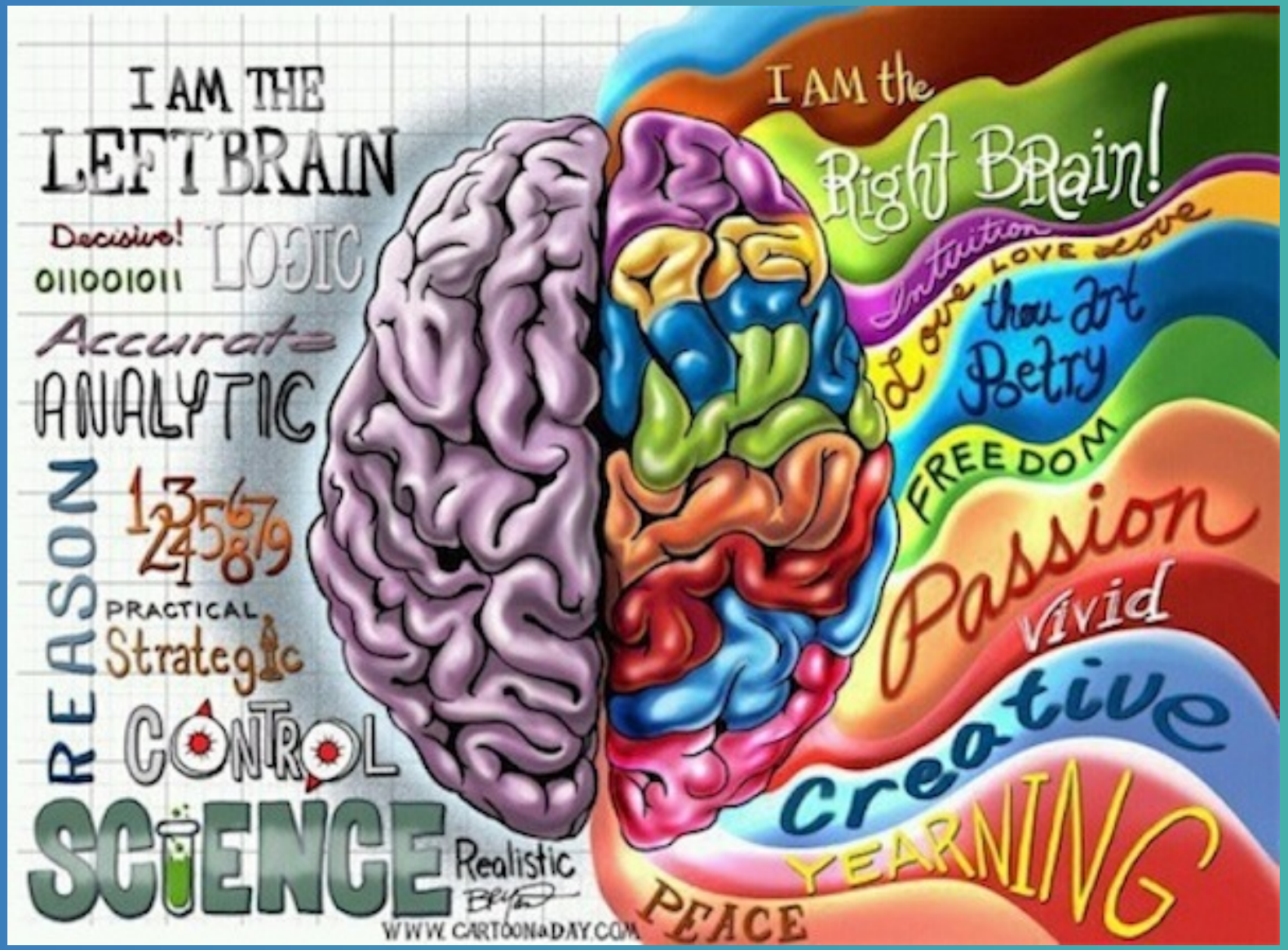
Security & Privacy are Solutions, not Problems

Better cybersecurity and (personal) data protection will enable new markets, promote innovation, and give consumers confidence to use new technologies that improve the quality of life.

Poor security will likely cause the Digital Technology markets to eventually collapse on itself as consumers, other users and society (the non-users) begin to lose trust in technology from compilations of digital disasters, social meddling and market failure.

AIOTI

Man & Technology Symbiosis: Hyperconnectivity!



Q&A: Anything Goes!

vanderwees@arthurslegal.com

aioti.eu
@aioti_eu

AIOTI