Privacy in IoT

The unique opportunity to learn and discuss where the Internet of Things meets GDPR, and where Hyperconnectivity meets Privacy & Security. Who wouldn't be totally confused!? In our Open Webinars, Arthur's Legal will address the Pains & Gains of the GDPR, X By Design & Resilience.


Arthur van der Wees


Dimitra Stefanatou


Janneke Breeuwsma

Arthur's Legal organizes seven (7) webinars on Privacy in IoT with the focus on GDPR, supported by AIOTI and Create-IoT

Go to **arthurslegal.com/iot/** for more information and subscription for the webinars.

ARTHUR'S LEGAL

Zapplied
Ignore us at your own peril

Privacy in IoT

Open Webinars by Arthur's Legal, supported by:

AIOTI WG3 Privacy-in-IoT Taskforce, and

H2020 CSA CREATE-IoT & LSPs AG Trust in IoT

Arthur van der Wees

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

Expert Advisor to the European Commission (Cloud, IoT, Data Value Chain, Cybersecurity, Privacy & Accountability)

Project Leader H2020 IoT LSPs & CSAs Activity Group on Trust, Security, Privacy, Accountability & Liability

Founding Member, EC's Alliance for IoT Innovation (AIOTI)

Task Force Leader AIOTI Security in IoT & Privacy in IoT

ARTHUR'S LEGAL

CREATE-IoT

European Large-Scale Pilots Programme

AIOTI ALLIANCE FOR INTERNET OF THINGS INNOVATION

Privacy in IoT Open Webinar Series

Webinar 1: GDPR: Processing, Protection, Security & Strategies

Webinar 2: X-by-Design: Upstream & Downstream Resilience

Webinar 3: State of the Art Privacy Principles & Requirements
Right Now!

Webinar 4: Consent Management & Engagement in IoT
Wednesday **2 May 2018**, 10.00 - 11.00 CET

Webinar 5: Compliance, Accountability, Assurance & Penalties
Wednesday **9 May 2018**, 10.00 - 11.00 CET

Webinar 6: IoT Ecosystems, Pre-Procurement & Collaboration
Wednesday **16 May 2018**, 10.00 - 11.00 CET

Webinar 7: Data Subject Rights & Data Management in IoT
Wednesday **23 May 2018**, 10.00 - 11.00 CET

ARTHUR'S LEGAL

Please subscribe to the Privacy in IoT Mailing List at: www.arthurslegal.com/IoT, in which we will keep you up to date with dates, login details and the latest news on the GDPR, Privacy in IoT and related topics.

CREATE-IoT

European Large-Scale Pilots Programme

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

Webinar Nr. 3

SOTA

State of the Art Privacy Principles & Requirements

CREATE-IoT

European Large-Scale Pilots Programme

AIOTI ALLIANCE FOR INTERNET OF THINGS INNOVATION

ARTHUR'S LEGAL

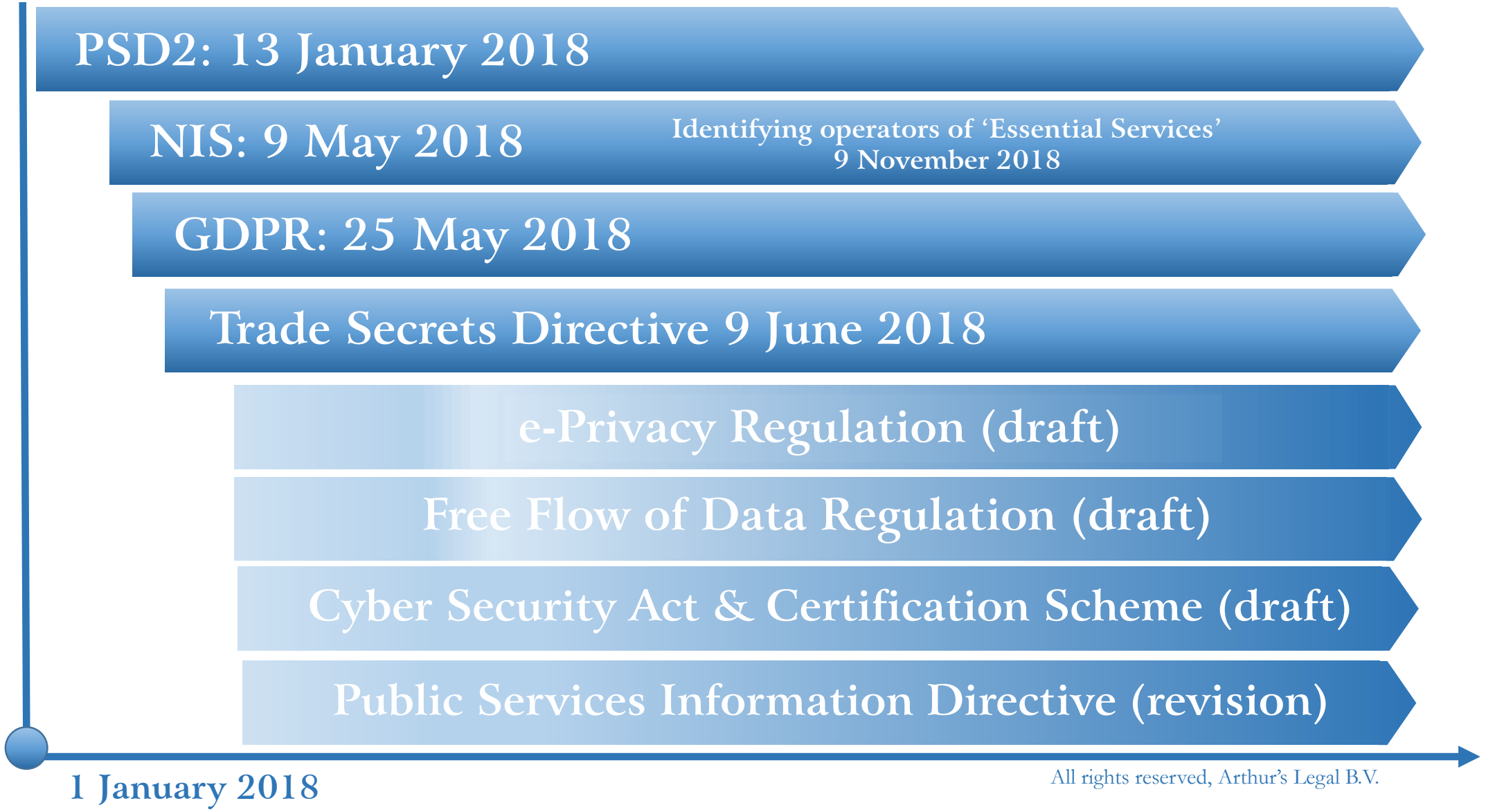
‘We are in a position today, in this Digital Age, where Technology has outstripped our Legal Framework’

Admiral Michael Rogers, Director NSA & Commander CYBERCOM

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

From 2018, Digital & Data become Highly Regulated Domains



30 Days

to Effective Date GDPR

25 May 2018

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

The GDPR is not reinventing the wheel …

ARTHUR'S LEGAL

Changes GDPR (Part 3 of 7)

Appropriate Personal Data Security Measures:

Appropriate Technical & Organizational Measures, Pseudonymisation & Encryption, Confidentiality, Integrity, Availability, Transparency, Isolation (Purpose Limitation), Data Intervenability, Monitoring & Evualuation

What Can We Do?

What Should We Do?

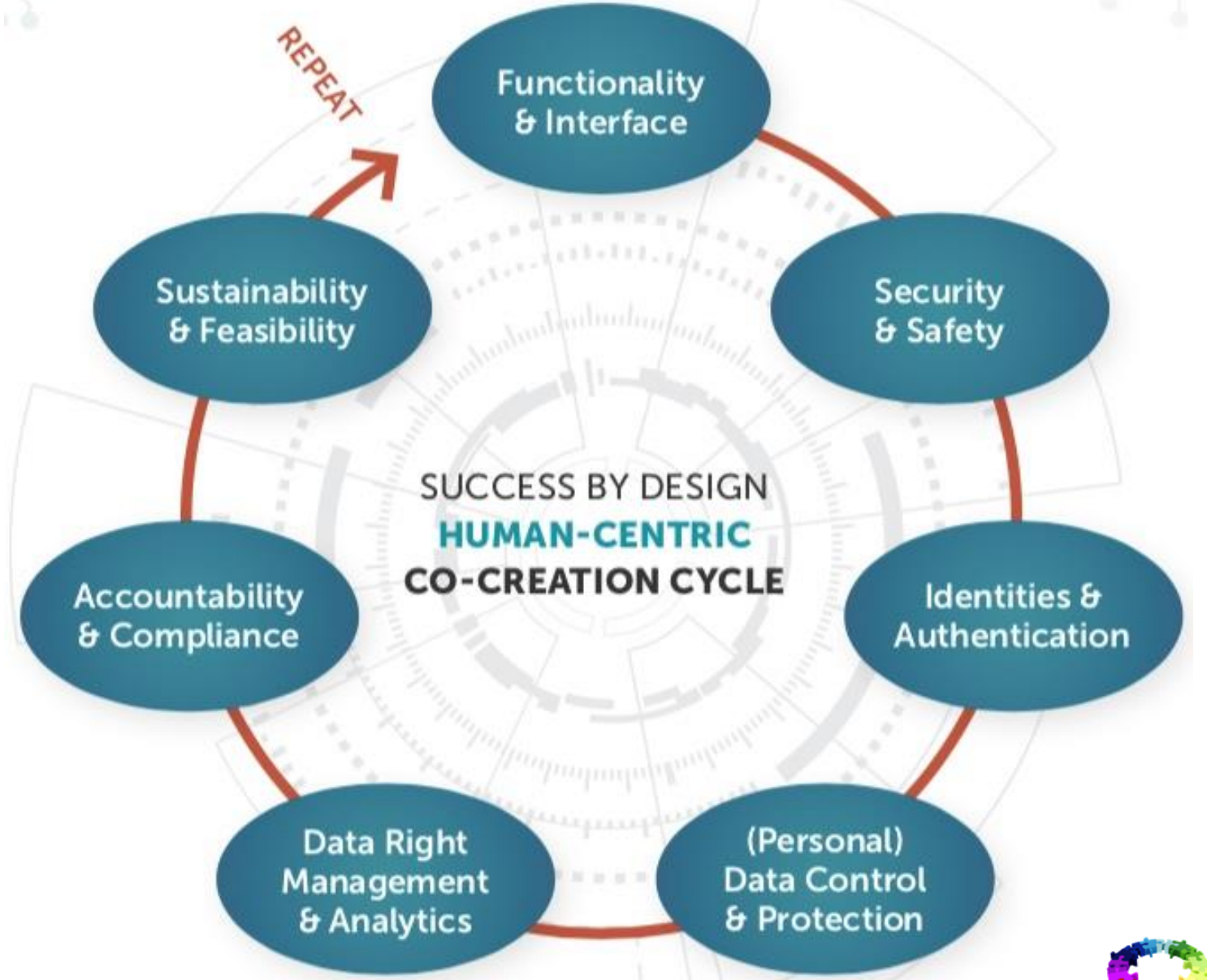
ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

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

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION



ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

All Markets Are Dynamic

#SOTA

State of The Art

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

Malicious Actors Are Not Into State of Play

State of the Art By Default & Daily Need

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

State of the Art

=

Principle-Based + Risk- & Impact-Based + Dynamic & Continuous

ARTHUR'S LEGAL

Principles & Requirements

Mandatory & Voluntary

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

GDPR =

GPDPMPS Regulation

Personal Data Collecting & Other Processing
Personal Data Protection & Security
Personal Data Management

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

First Privacy Principle in IoT

No Personal Data by Default

Avoid Personal Data (PII) Collection or Creation (*)

(*) Exceptions permitted, when & where required

ARTHUR'S LEGAL

Second Privacy Principle in IoT

‘As If’ X-By-Design

Design & Engineer Ecosystems As-If these will (now or in a later phase) process Personal Data

Privacy & Security By Default & By Design

ARTHUR'S LEGAL

Privacy by Default

vs

Security by Default

ARTHUR'S LEGAL

Privacy & Security Principles in IoT

Data Minimisation

ARTHUR'S LEGAL

Privacy & Security Principles in IoT

Purpose Limitation

No legal ground or legitimate interest under the GDPR, no more data processing

ARTHUR'S LEGAL

Privacy & Security Principles in IoT

De-Identifying & Data Deletion

The fine balance between immediate strong deletion when no legal ground and legitimate purpose under the GDPR is available, and mandatory retention obligations by the data controller/processor.

ARTHUR'S LEGAL

Privacy & Security Principles in IoT

Transparency

A data subject should be able to know who is taking what action with its personal data

ARTHUR'S LEGAL

Privacy & Security Principles in IoT

Data Control

A data subject should at all times be able to have control over its personal data.

ARTHUR'S LEGAL

Privacy & Security Principles in IoT

Accountability

Any data controller/processer is accountable for regulatory and contractual compliance to the extent concerning its level of collecting, using, sharing and other processing, the related impact assessement linked to technical and operational measures, including with and for data subcontractors involved. Accountability can not be outsources.

ARTHUR'S LEGAL

Minimise Fragmentation

Source: AIOTI WG3 (IoT Standardisation) – Release 2.7

ARTHUR'S LEGAL

Build Your Own SOTA Security in IoT Model

It's Easy; Just Think N-Dimensional!

1. 35+ SOTA Security Recommendations, Frameworks & Guidelines
2. 1.000+ Security Requirements & Principles (450+ Unique)
3. Segmentation into 4 Layers & 3 Dimensions
4. Structure, Systemize & Semantic Sanitization without Interpretation
5. Context (initially: each of the 5 LSPs)
6. Stakeholders (User, Customer, Supplier, Policy Makers, SDO, Authorities)
7. 5 Life Cycle Metholodogies (Device, Data, Stakeholder, Context, Legal)
8. Interdependencies & Double-Looping

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

GDPR Stakeholders

- Data Subject
- Data Controller
- Data Processor
- Data Protection Authority
- Other Data Actors

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

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

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

General IoT Layered SOTA Plotting Methodology:

Dimensions & Layers

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

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

7 Phases of the (Personal) Data Life Cycle

Which phase(s) are we talking about?
PII* + Actor + Legal Basis + Purpose(s)

1. Obtain /Collect
2. Create / Derive
3. Use
4. Store
5. Share / Disclose
6. Archive
7. Destroy / Delete

Most PII* comes out of Phase 1 & 2

BUT

Personal Data is created & processed in any and each phase

ARTHUR'S LEGAL

* PII: personal identified or identifiable information

Continuous SOTA Security

State of the Art Security 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.

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

From Continual to Continuous State of the Art Security

Although the current information security standards aim for '**achieving continual improvement**', articles 25 and 32 GDPR aims to ensure up-to-date levels of protection by requiring the levels of data protection and security to **continuously** meet the Appropriate Dynamic Accountability (ADA) Formula

State of the Art Security – Costs – Purposes + Impact

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

Security & Privacy in IoT / State of the Art (SOTA)

1. European Commission (EC) & Alliance for Internet of Things Innovation (AIOTI): Report on Workshop on Security & Privacy in IoT (2016 & 2017)
2. Alliance for Internet of Things Innovation (AIOTI): Report on Workshop on Security and Privacy in the Hyper-Connected World (2016)
3. European Commission (EC): Best available techniques reference document for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems (2016)
4. European Union Agency for Network and Information Security (ENISA): Auditing Security Measures (2013)
5. European Union Agency for Network and Information Security (ENISA): Cloud Certification Schemes Metaframework (2014)
6. Energy Expert Cyber Security Platform: Cyber Security in the Energy Sector (2017)
7. HM Government, Department for Transport and Centre for the Protection of National Infrastructure: The Key Principles of Cyber Security for Connected and Automated Vehicles (2017)
8. Autorité de régulation des communications électroniques et des postes (ARCEP): Preparing for the internet of things revolution (2016)
9. United States Department of Commerce (DoC): Fostering the advancement of the Internet of Things (2017)
10. United States Department of Homeland Security: Strategic Principles for Securing the Internet of Things (2016)
11. United States Department of Health and Human Services, Food and Drug Administration: Postmarket Management of Cybersecurity in Medical Devices (2016)
12. United States Department of Health and Human Services, Food and Drug Administration: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
13. United States Government Accountability Office: Technology Assessment: Internet of Things – Status and implications of an increasingly connected world (2017)
14. National Institute of Standards and Technology (NIST): Networks of 'Things' (2016)
15. IoT Alliance Australia (IoTAA): Internet of Things Security Guideline (2017)
16. GSM Association (GSMA): IoT Security Guidelines Overview Document (2016)
17. GSM Association (GSMA): IoT Security Guidelines for Service Ecosystems (2016)
18. GSM Association (GSMA): IoT Security Guidelines for Endpoint Ecosystems (2016)
19. GSM Association (GSMA): IoT Security Guidelines for Network Operators (2016)
20. IoT Security Foundation (IoTSF): IoT Security Compliance Framework (2016)
21. IoT Security Foundation (IoTSF): Connected Consumer Products Best Practice Guidelines (2016)
22. IoT Security Foundation (IoTSF): Vulnerability Disclosure (2016)
23. Broadband Internet Technical Advisory Group (BITAG): Internet of Things (IoT) Security and Privacy Recommendations (2016)
24. International Organization for Standardization (ISO): Internet of Things Preliminary Report (2014)
25. The Center for Internet Security (CIS): Critical Security Controls v6.0 (2016)

35 +

Regulatory Technical Standards of Payment Services Directive (2017)
US Congress Proposal for IoT Cybersecurity Improvement Act (2017)
Online Trust Alliance: IoT Security & Privacy (2017)
OWASP IoT Framework Assessment (2018)

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

Security in IoT / State of the Art (SOTA)

EC/AIOTI Reports on Workshops on Security and Privacy in IoT

AIOTI Workshop on Security and Privacy in IoT of June 2016:
https://ec.europa.eu/digital-single-market/en/news/aioti-workshop-security-and-privacy-etsi-security-week

Final Report Workshop on Security and Privacy in IoT of June 2016:
https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf

Final Report European Commission of January 2017 Workshop on Internet of Things Privacy and Security:
https://ec.europa.eu/digital-single-market/en/news/internet-things-privacy-security-workshops-report

IERC IoT Handbook Paragraph 6.3.3:
http://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609105C6.pdf

Snapshot Example
SOTA Security Plotting

		10.1	10.2	10.3	10.4	10.5
287	Network authentication			Y		Y
288	Device and owner authentication					
289	Utilize a trust anchor			Y		Y
290	Use a tamper resistant trust anchor			Y		
291	Enforce confidentiality and integrity to/from the trust anchor			Y		
292	Perfect Forward Secrecy (PFS)			Y		
293	Force authentication through the service ecosystem		Y			
294	Define application layer authentication and authorisation		Y			
295	Define an organizational root of trust		Y	Y		Y
296	Define a communications model		Y			

10.01 GSMA: IoT Security Overview Document
10.02 GSMA: IoT Security Guidelines for IoT Service Ecosystem
10.03 GSMA: IoT Security Endpoint Ecosystems
10.04 GSMA: IoT Security Guidelines for Network Operators
10.05 GSMA: IoT Security Assessment Framework

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

Contextuality

ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

Use Case: Smart Carpets

ARTHUR'S LEGAL

ACTIVAGE PROJECT

www.activageproject.eu

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

General State of The Art SOTA IoT Plotting Methodology

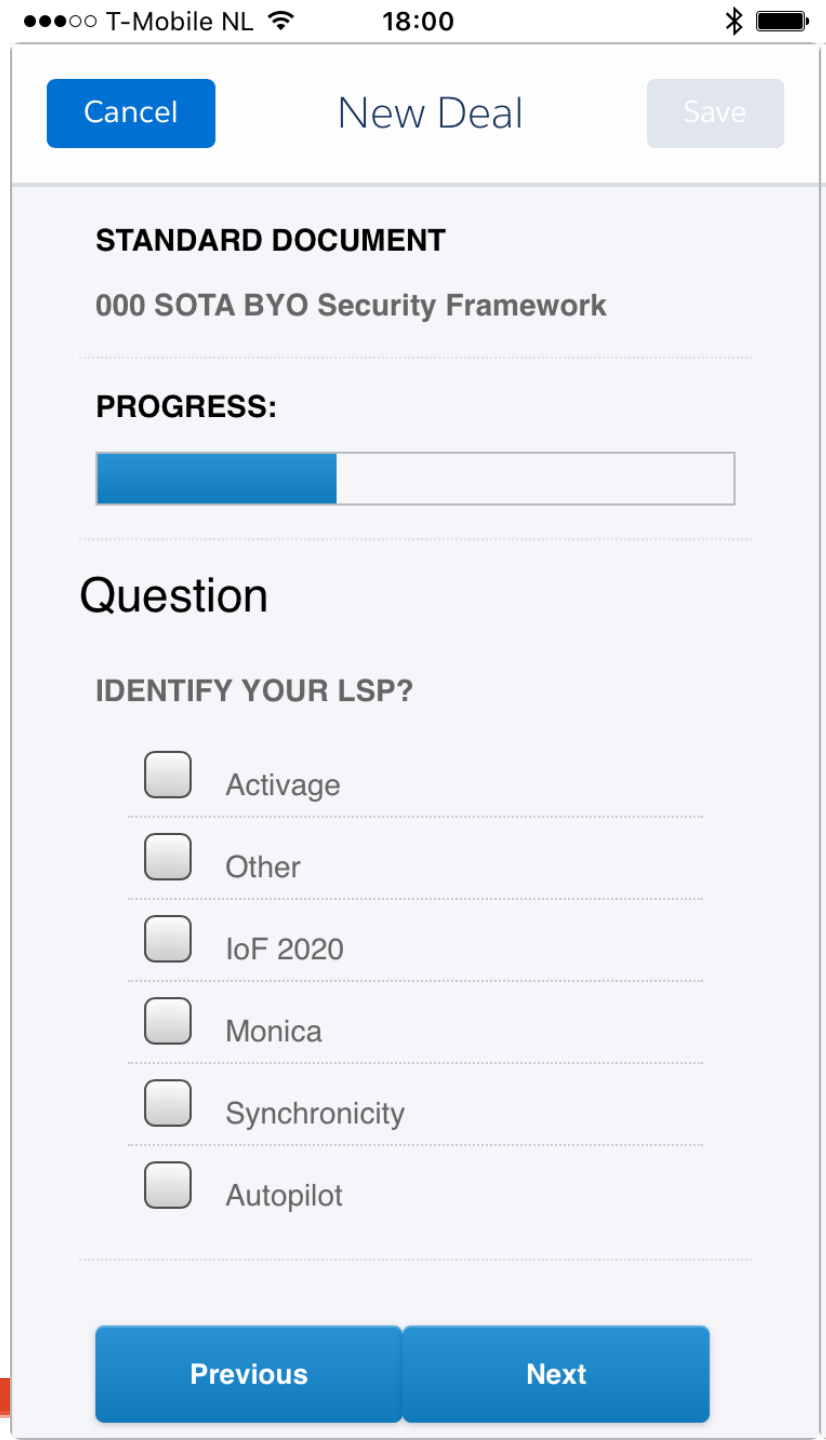
1. User/Human Factor
2. Data
3. Service
4. Software/Application
5. Hardware
6. Authentication
7. Infrastructure/Network

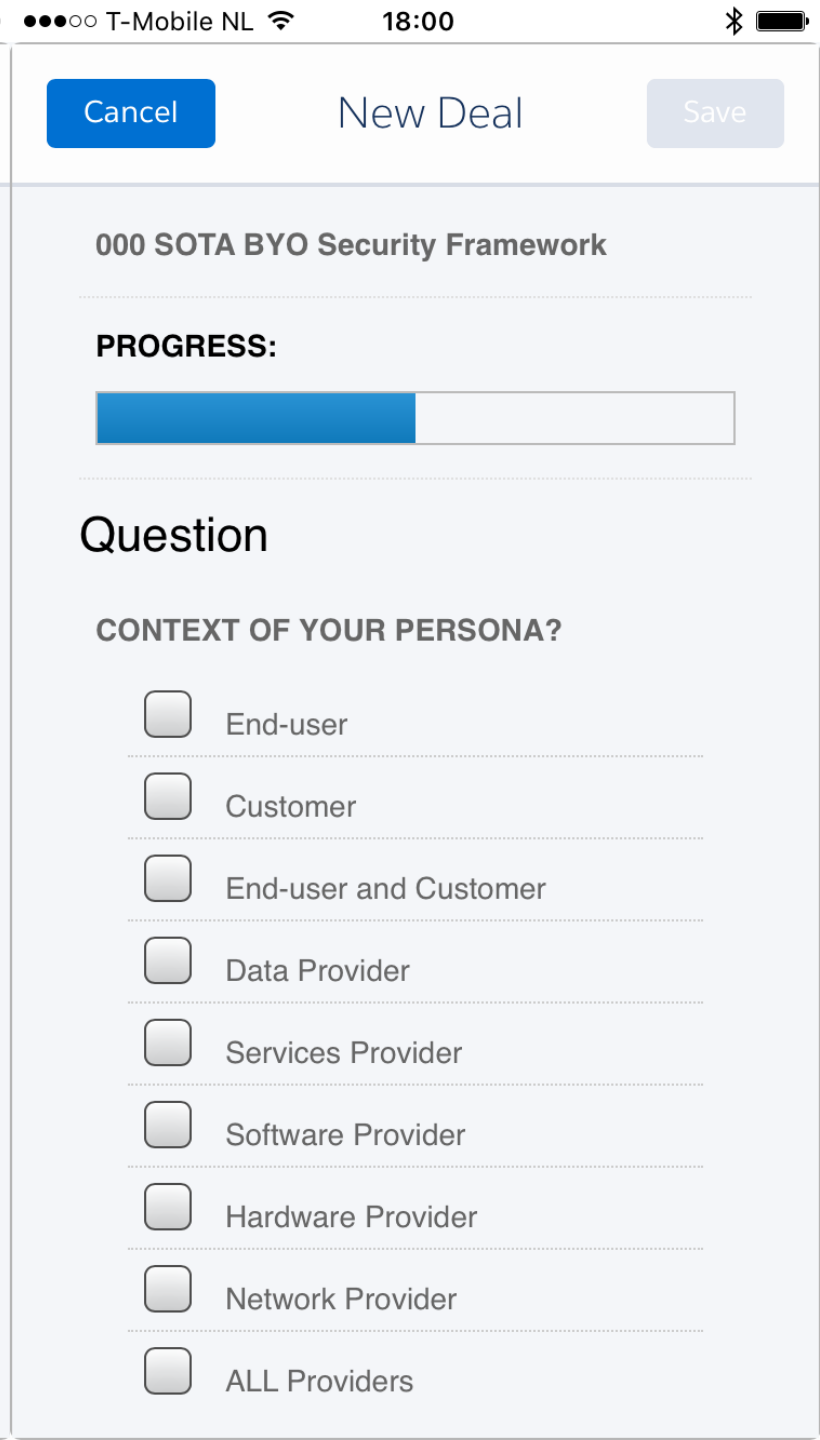
ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

Use Case 1: Smart Carpet Sensors for Aging Well

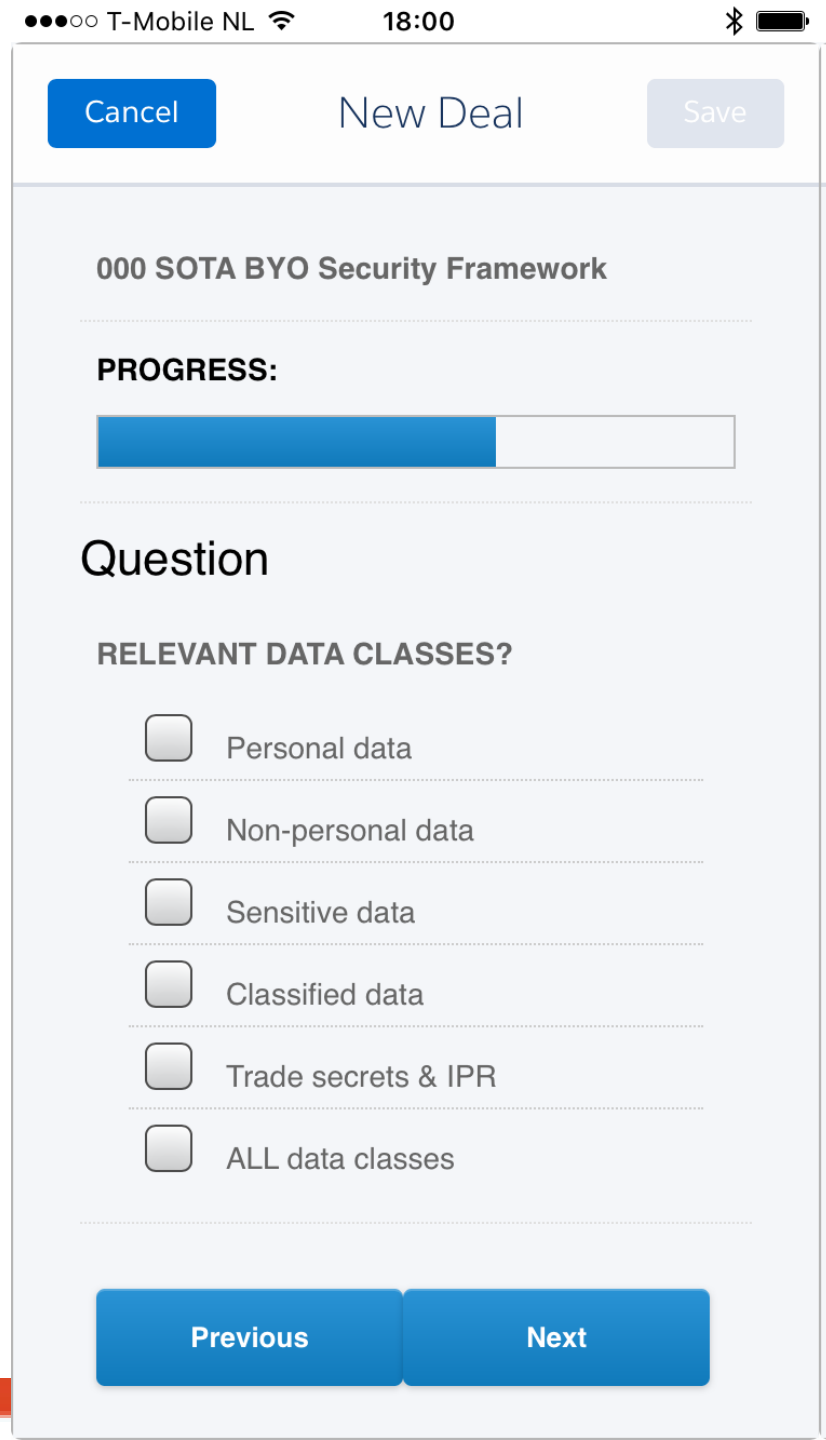
ARTHUR'S LEGAL

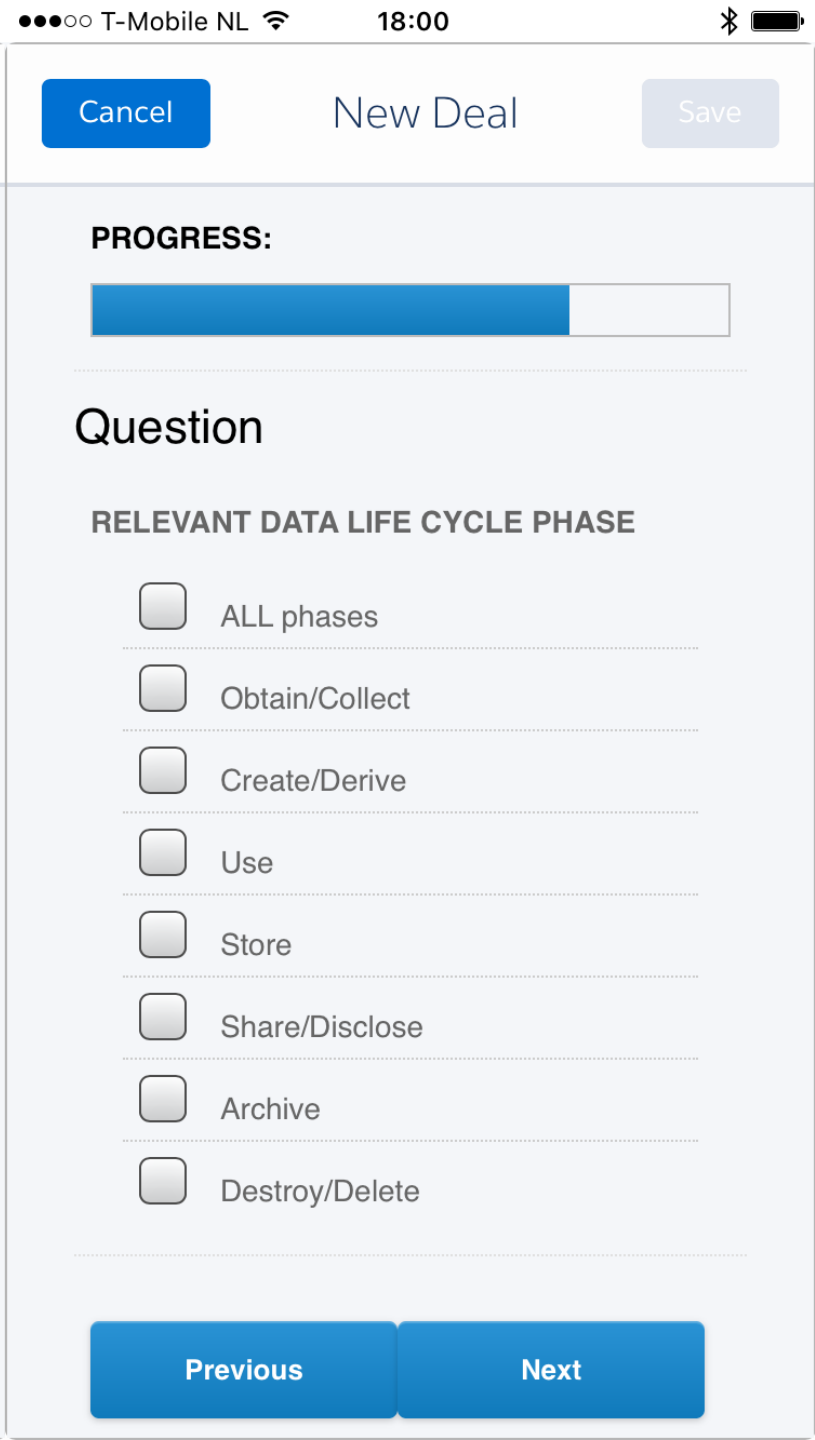




Use Case 1: Smart Carpet Sensors for Aging Well

ARTHUR'S LEGAL





Use Case 1:

Smart Carpet Sensors for Aging Well

ARTHUR'S LEGAL

1. **USER/HUMAN FACTOR**
    1. **Basic principles:**
        1. Human-centric approach: Security and privacy should be universally applied to all users.
        2. Privacy by design: Privacy of users must be embedded into the design of business processes, technologies, operations and information architectures. Each service or business process designed to use personal data must take all the necessary security requirements into consideration at the initial stages of their developments. Privacy must be embedded into the design of business processes, technologies, operations and information architectures.
        3. Privacy by default: The strictest privacy settings and mechanisms must automatically apply once a user acquires a new product or service; no manual change to the privacy settings should be required on the part of the user.
        4. Decoupling multiple identities: It should be easy to decouple multiple personae of the users from one another.
    2. **User's awareness and control:**
        1. Transparency of data processing: The service provider should empower users to know what the devices are doing and what personal data they are sharing and why, even if it concerns M2M communications and transactions.
        2. Transparency of privacy policy: The service provider should ensure that the user is and remains clear and aware of privacy issues, choices it makes and possible consequences thereof.
    3. **Handling of personal data:**
        1. Non-discriminatory practices: The service provider should ensure non-discriminatory practices against users and businesses on the basis of information derived from IoT deployments (e.g. within smart cities).
        2. Manufacturer-implemented parametrization: By design, the user should be able to configure and manage rights for accessing data controlled by them based on the assessment where (in its lifecycle) the device comes into contact with personal data, creates/derives (new) personal data, or otherwise processes personal data, while keeping in my mind the contextuality of purposes and use, as well as multi-purpose Things and IoT ecosystems.
        3. Accountability: Any service provider should be accountable for regulatory, contractual and ethical compliance.

Use Case 1:

Smart Carpet for Aging Well

6. AUTHENTICATION

Location authentication

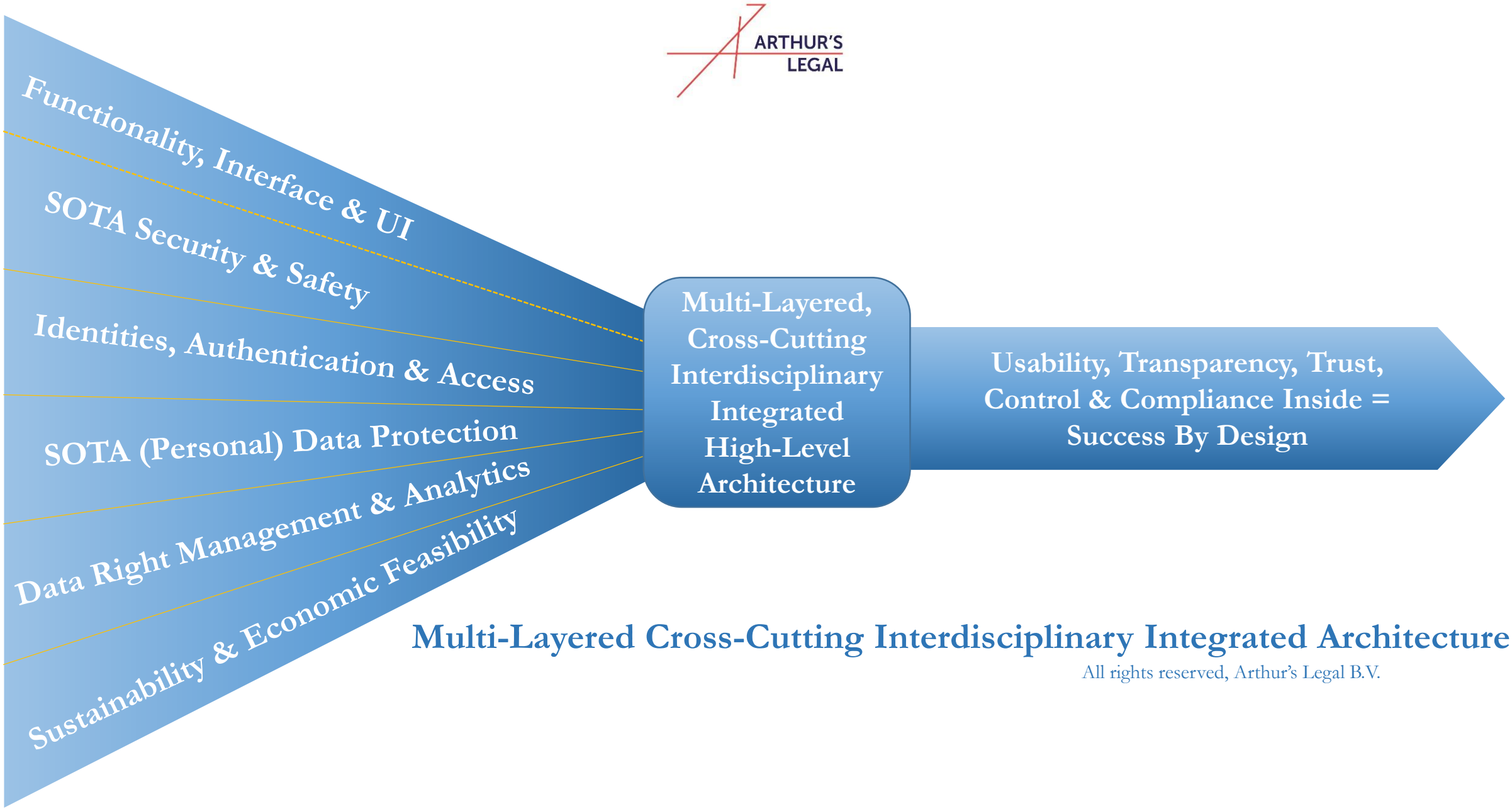
Network authentication

7. INFRASTRUCTURE/NETWORK

System tests & assurance

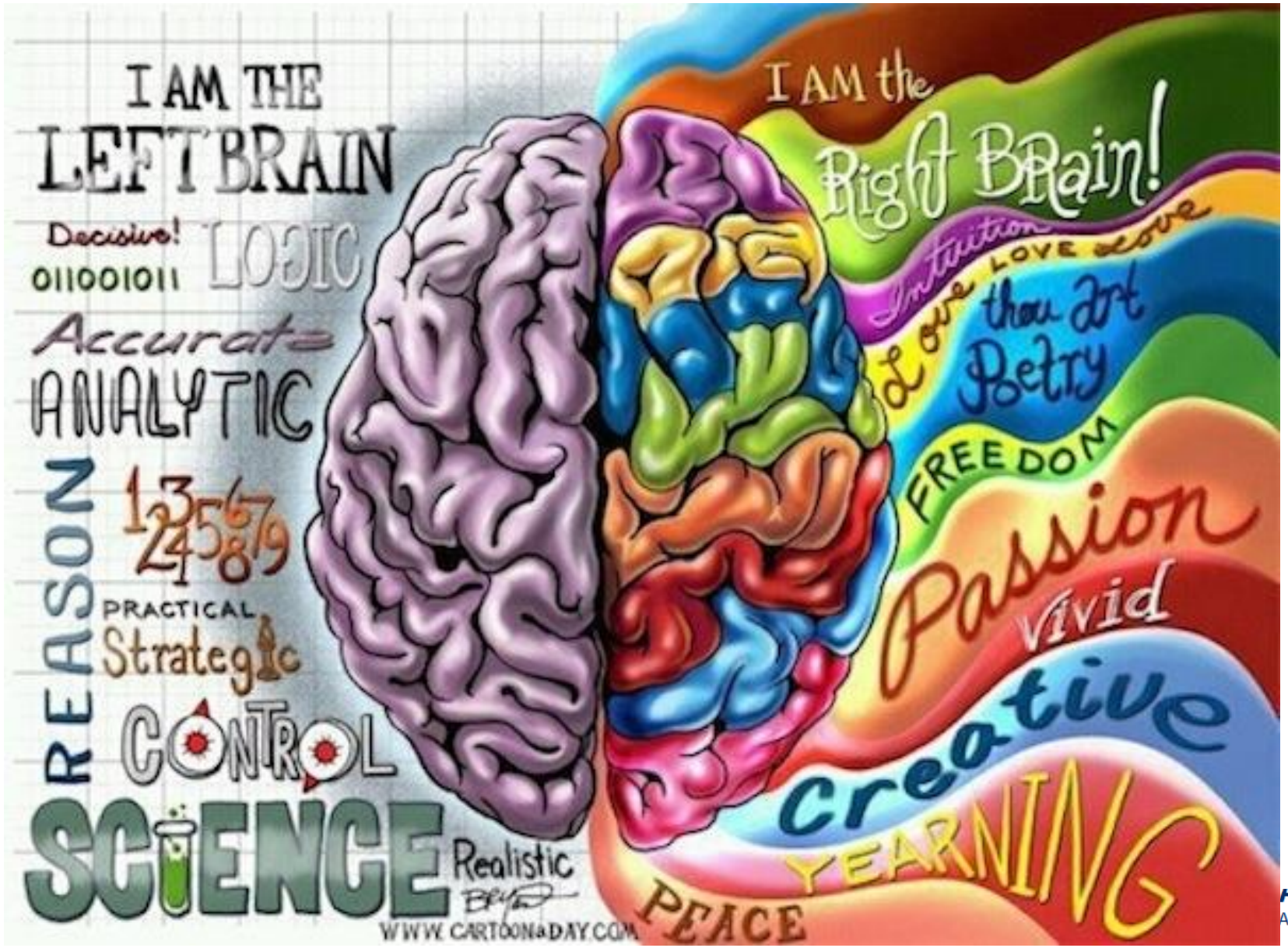
ARTHUR'S LEGAL

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION



Multi-Layered Cross-Cutting Interdisciplinary Integrated Architecture

Man & Technology Symbiosis: Hyperconnectivity!



Q&A: Anything Goes!

vanderwees@arthurslegal.com

Arthurslegal.com
@Arthurslegal

ARTHUR'S LEGAL

ALLIANCE FOR INTERNET OF THINGS INNOVATION

Arthur's Strategic Services & Systems } Global Tech & Strategies by Design. Est. 2001

Arthur's Legal: Arthur's Legal a global tech and strategic x-by-design law firm. Arthur's Legal is founded in 2001 and since its incorporation provides integrated full services, and mainly focuses on local and global private and public organizations that are active as customer, user, vendor, integrator, consultant, legislator or policy maker in the fields of IT, licensing, cloud computing, internet of things, data analytics, cybersecurity, robotics, distributed ledger (block chain) technology and artificial intelligence. Arthur's Legal is also a leading deal making expert; it has already structured and negotiated out more than 5.000 major technology and related deals with and for global Fortune companies as well as other major organizations in the public and private sector worldwide.

Arthur's Global Digital Strategies: The counsels of Arthur's Legal are legal experts, strategists, technologists, standardization specialists and frequent speakers worldwide, with in-depth experience and are well-connected in the world of technology, combinatoric innovation, data, digital, cybersecurity, (personal) data protection, standardization, risk management & global business. On these topics, its managing director Arthur van der Wees LLM is expert advisor to the European Commission, Dutch government as well as other public and private sector organizations and institutes worldwide.

Trust, Digital Data, Cybersecurity, Algorithms, AI, Robotics & Internet of Things: Arthur's Legal is Founding Member of European Commission's (EC) Alliance of IoT Innovation (AIOTI), Co-Chair of AIOTI WG4 (Policy), Project Leader of both the AIOTI Security in IoT and Privacy in IoT taskforces, co-author of EC's Cloud SLA Standardisation Guidelines, co-author of Cloud Security Alliance's Privacy Level Agreement (PLA) 2.0, co-contributor to ISO standards such as ISO/IEC 19086 (Cloud Computing), co-author of the IERC Handbooks 2016 (Strategic & Legal Challenges in IoT) and 2017 (Security & Privacy in IoT), member of ESCO and co-author of the Dutch National Smart Cities Strategy. Arthur's Legal is co-founder of CloudQuadrants on the maturity of cloud offerings, the Cyberchess Institute that landscapes the real-life cybersecurity arena, the Cyber Trust Institute that sets trust trajectories and orbital requirements and parameters for technology-as-a-service, the Institute for Next Generation Compliance that promotes the restructuring and automation of compliance and related procurement, and the Institute for Data and Evidence Based Trust that aims to build and enhance trust and data protection in open, decentralized digital, cyber-physical and virtual ecosystems. Furthermore, Arthur's Legal is EC H2020 project IoT CREATE consortium partner and activity group leader on trust, security, safety, privacy, legal and compliance topics in IoT in five EU large scale pilots on smart healthcare, smart cities, wearables, smart farming, food safety and autonomous vehicles with EUR 250M of accrued EC and other funding. Together with IDC Arthur's Legal is also doing research and policy making for the Commission on data portability & application portability. One can build it's own AI with Zapplied.

Connected & Hyper-connected: Arthur's Legal has an unique interdisciplinary 3D-angle & x-by-design approach, connecting vital topics such as usability, security, data management, (personal) data protection, compliance with technology, infrastructure, architecture and global standardization thereof, with the capability and ability to connect those components in hyper-connected ecosystems much earlier (read: pro-active, preventative) than the traditional policy-making, legal and compliance practice does. For upcoming events, key notes and other activities, please check out website, stay up to date via its social media channels, or contact us.

Zapplied
Ignore us at your own peril

www.arthurslegal.com | vanderwees@arthurslegal.com

ARTHUR'S LEGAL

Trustworthy Internet of Everything & Everybody for the Wellbeing of People and Planet

Legal Notices