

IT'S THEIR
RESPONSIBILITY
FIRST.

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.



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
Mrs. Janneke Breeuwsma LLM

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



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

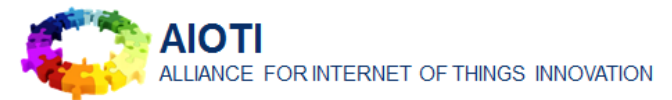
Webinar 4: Consent Management & Engagement in IoT

Webinar 5: Compliance, Accountability, Assurance & Penalties

Webinar 6: IoT Ecosystems, Pre-Procurement & Collaboration

Webinar 7: Data Subject Rights & Data Management in IoT

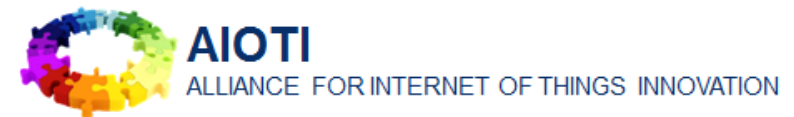
Please subscribe to the Privacy in IoT Mailing List at: www.arthurslegal.com/IoT, in which we will keep you up to date with dates, login details and the latest news on the GDPR, Privacy in IoT and related topics.



2 Days

to Effective Date GDPR

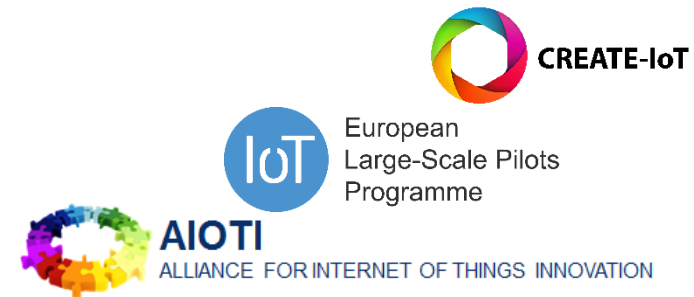
25 May 2018



Privacy in IoT

Webinar Nr. 7

Data Subject Rights & Data Management in IoT



#Giving Privacy Back

What can we do?

What should we do?

Data Subject Consent

The data subject should be informed of the data processing, the purpose thereof, the identity of the data controller(s) and all other information necessary for fair processing. In some cases they even have to give explicit consent to the processing of Personal Data, this depends on the justification grounds and is always the case when processing sensitive data.






















The consent should be:

1. Freely given
2. Specific
3. Informed
4. A clear and unambiguous indication of a data subject's wishes

Data Collection Modalities:

- A. Concise
- B. Easily accessible
- C. Easy to understand
- D. Where appropriate visualized
- E. Clear & plain language (also, for information addressed to children)
- F. No ambiguity

Achieving informed and explicit consent difficult

							
	Facebook	Instagram	LinkedIn	Snapchat	Twitter	Happn	Tinder
Total number of Words (average 5700)	6 208	7 636	11 838	6 848	6 841	4 343	8 399
Total number "may" / "can" (average 59,3)	32	107	138	77	77	20	85
Clear language							
Efforts to make readable							

Data Management

1. Right to Notice

2. Right to Object

(& Right to Object to Automated Decision Making & Profiling)

3. Right to Access

4. Right to Rectify

5. Right to Data Portability

6. Right to be Forgotten

Sanctions in case of non-compliance to (for instance) Data Subject Rights and Transfer of Personal Data

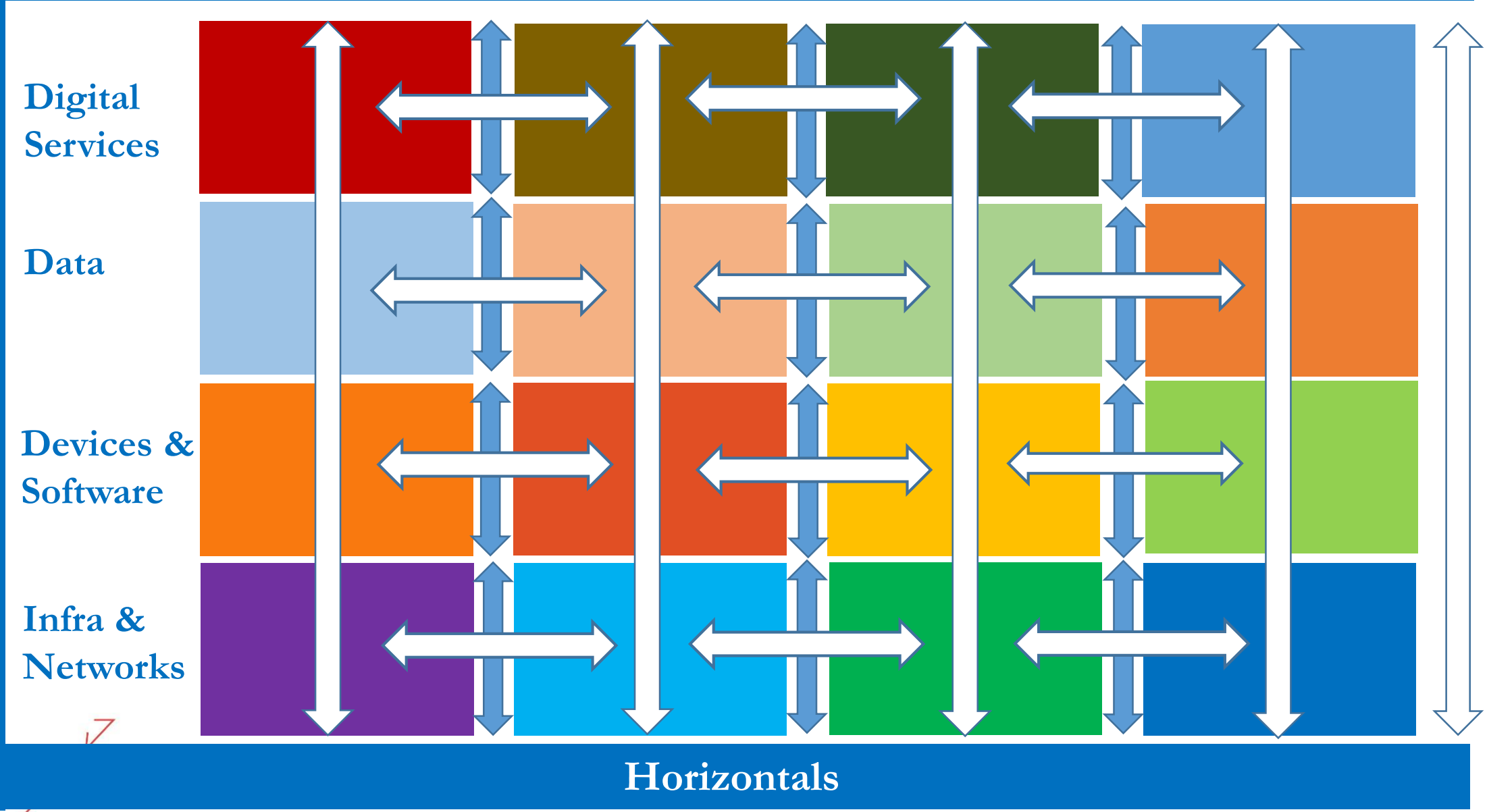
Failure to meet the above requirements exposes the **organisation** to an administrative fine of **up to EUR 20.000.000**, or in case of an undertaking up to **4%** of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Data Control Data Access Use & DRM

Data Management within IoT?

Hyperconnected, accountable Value Chain towards the Customer: B2x, G2x, C2x

Vertical & Horizontal Value Chains



Right to Notice

(article 13 GDPR)

Information to be provided where the
Personal Data are collected from the
Data Subject before processing

The controller has to inform Data Subjects about:

1. The identity and contact details of the controller or its data protection officer
2. If their personal data are processed
3. Why is processing takes place
4. Any other information necessary (circumstances & context of processing)
5. If the data is or will be transferred to a third country outside the EU, without the appropriate safeguards
6. If mandatory to give personal data, consequences if not

**In Practice the Right to Notice
(also the other data subject
rights) will be included in the
Privacy Policy**

Right to Object

(article 21 GDPR)

(& Right to Object to Automated
Decision Making & Profiling)

Right to Object

- Relating to a particular situation of the Data Subject
- At any time
- When Processing is based on the legal ground (a) Public interest or (b) Legitimate Interest of the Data Controller, including profiling
- Than, no longer process the personal data,
- Unless controller demonstrates legitimate grounds which override the interests, rights and freedoms of the data subject, establishment, exercise or defense of legal claims.
- When direct marketing purposes are involved, than right to Object at any time, including profiling

Right to Access

(article 15 GDPR)

A. Right to obtain confirmation
whether personal data are
processed or not



B. Specific information

- a. purposes of processing,
- b. categories of personal data,
- c. recipients to whom the personal data will be disclosed,
- d. the envisaged period of storage,
- e. the right to request rectification or erasure of personal data,
- f. the right to lodge a complaint by a supervisory authority,
- g. any available information to the source when not collected the personal data directly from the data subject and existence of profiling.

Right to Rectification

(Article 16 GDPR)

The data subject shall have the right to obtain from the controller without undue delay the **rectification of inaccurate** personal data

Taking into account the purposes of the processing, the data subject shall have the right to have **incomplete personal data completed**.

The right to change one's mind is reflected not only on withdrawal of consent, but also, on the right to data portability

Right to Data Portability

(Article 20 GDPR)

- The Data Subject shall have the right to receive his/her Personal Data
- In a **structured, commonly used and machine-readable format**
- The right to transmit those Personal Data to another controller without hindrance
- The right to transmit those directly from one controller to another, where technically feasible
- Without prejudice to the right to be forgotten

Does Data Portability imply Data Deletion?

Right to be Forgotten

(Article 17 GDPR)

A. The data subject shall have the right to obtain **the erasure** of his/her personal data, without undue delay

B. The controller shall have the obligation to erase personal data without undue delay when, i.e.:

- Personal Data are **no longer necessary** related to the purpose
- The data subject **withdraws consent**
- Data Subject **objects** to the processing
- Personal Data is **unlawfully processed**

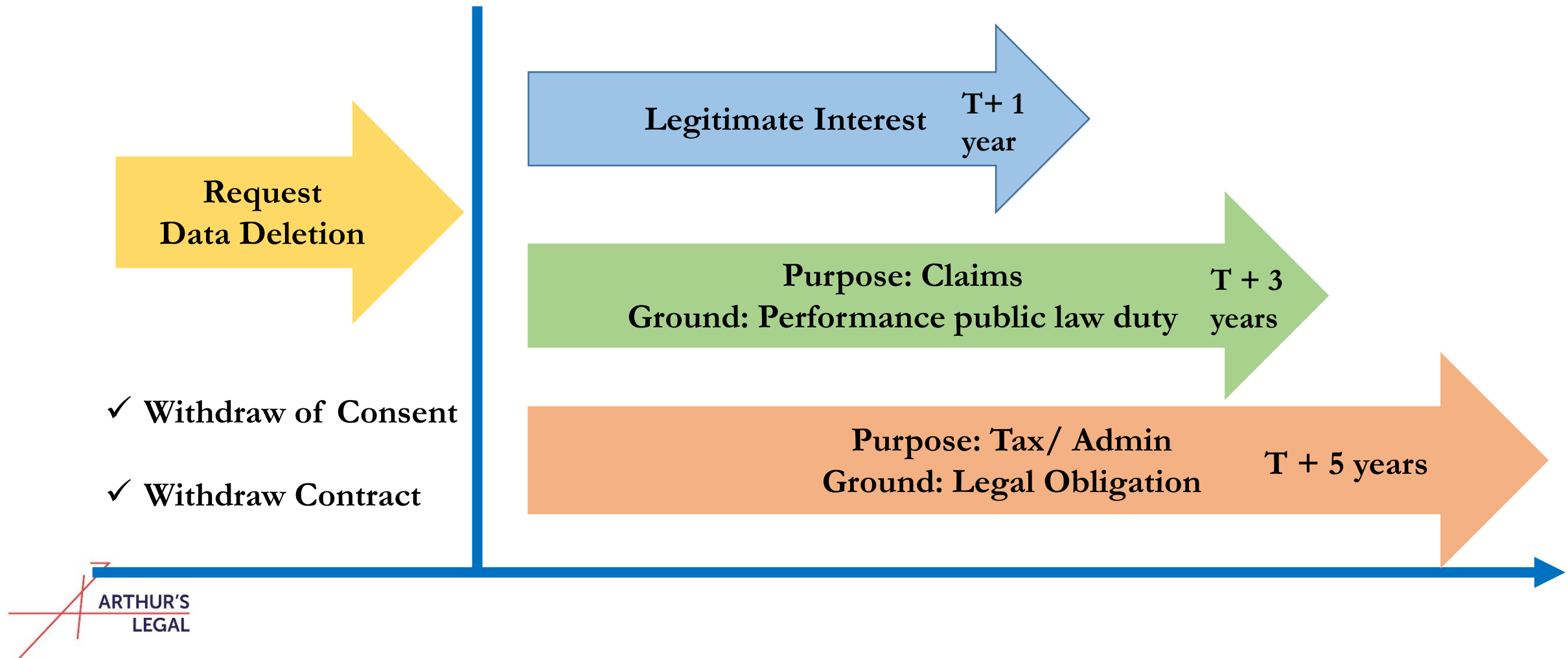
Relevant for all Data Subject Rights:

1. Time of reaction by controllers:

With undue delay and in any event within one month of receipt of the request (with possibility extend for another two months)

2. Derogations by EU or Member States law

Request vs Mandatory Data Retention



Justification Grounds = The Sole Window

1. **Unambiguous Consent:** Freely given specific and informed
2. **Performance of a contract:** Necessary for the performance of an Agreement with the data subject in question
3. **Legal Obligation:** Comply with a legal obligation
4. **Protecting vital interests of the data subject**
5. **Performance of a public law duty:** By an administrative body
6. **Legitimate Interest:** The legitimate interest of the controller or recipients of the personal data , only when the fundamental rights and freedom of the data subject would not prevail.

From 2018, Digital & Data become Highly Regulated Domains

PSD2: 13 January 2018

NIS: 9 May 2018

Identifying operators of 'Essential Services'
9 November 2018

GDPR: 25 May 2018

Trade Secrets Directive 9 June 2018

e-Privacy Regulation (draft)

Free Flow of Data Regulation (draft)

Cyber Security Act & Certification Scheme (draft)

Public Services Information Directive (revision)

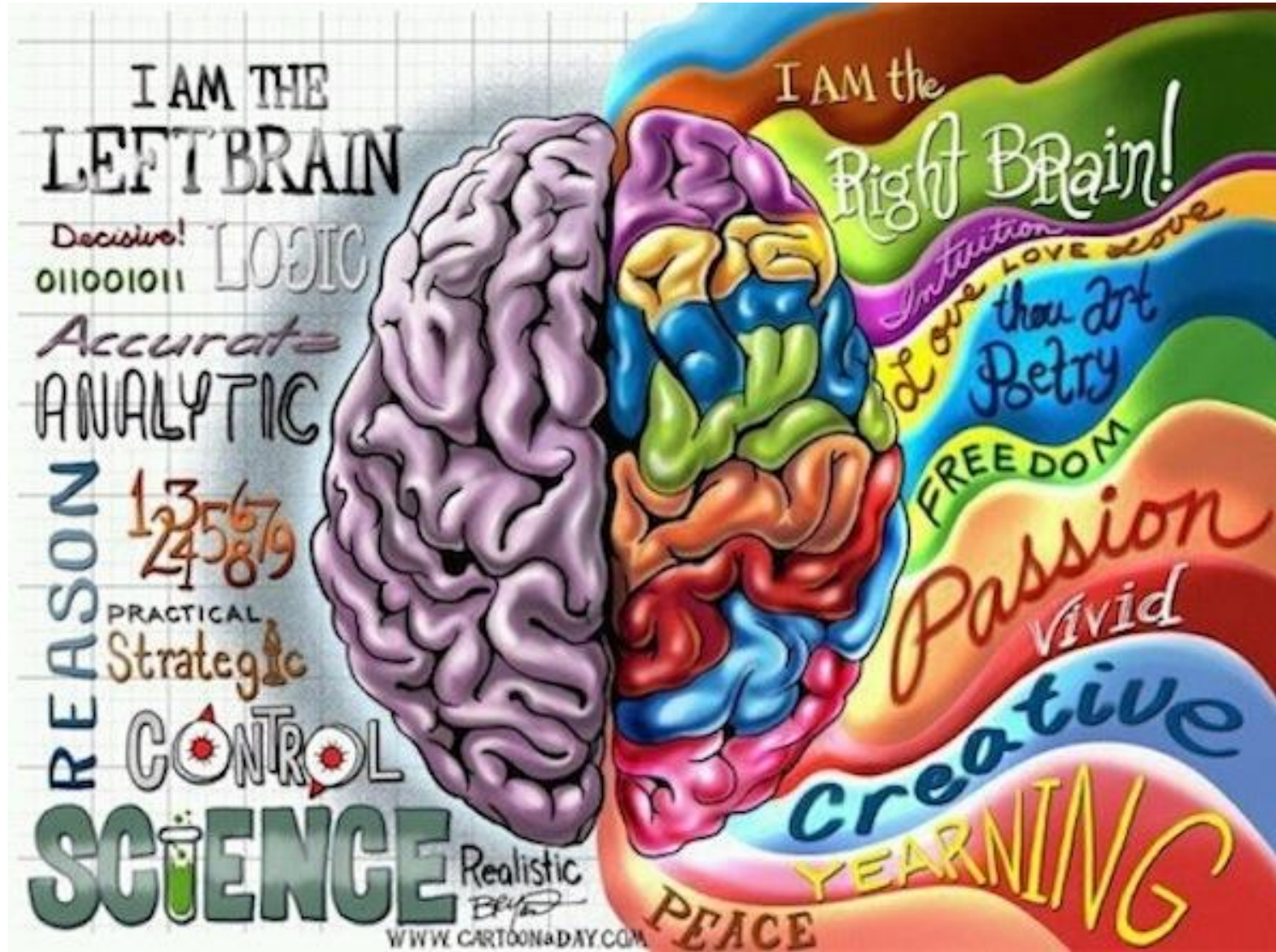
1 January 2018

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

What's next?

Please elaborate!

Man & Technology Symbiosis: Hyperconnectivity!



Q&A:
Anything
Goes!

breeuwsma@arthurslegal.com

Arthurslegal.com
[@Arthurslegal](https://www.instagram.com/Arthurslegal)

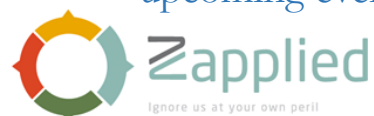
Arthur's Strategic Services & Systems } Global Tech & Strategies by Design. Est. 2001

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.



www.arthurslegal.com | vanderwees@arthurslegal.com





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

Legal Notices

All rights reserved, Arthur's Legal. The content of this document is provided 'as-is' and for general information purposes only; it does not constitute strategic, legal or any other professional advice. The content or parts thereof may not be complete, accurate or up to date. Notwithstanding anything contained in this document, Arthur's Legal disclaims responsibility (including where Arthur's Legal or any of its officers, employees or contractors have been negligent) for any direct or indirect loss, damage, claim, or liability any person, company, organisation or other entity or body may incur as a result, this to the maximum extent permitted by law.