CLOUD DATA PRIVACY - GDPR

Aleksandar Bratic

CSA cloud security alliance®

OUR COMMUNITY

84,000+
INDIVIDUAL MEMBERS

75+
CHAPTERS

300+
CORPORATE MEMBERS

34+
ACTIVE WORKING GROUPS

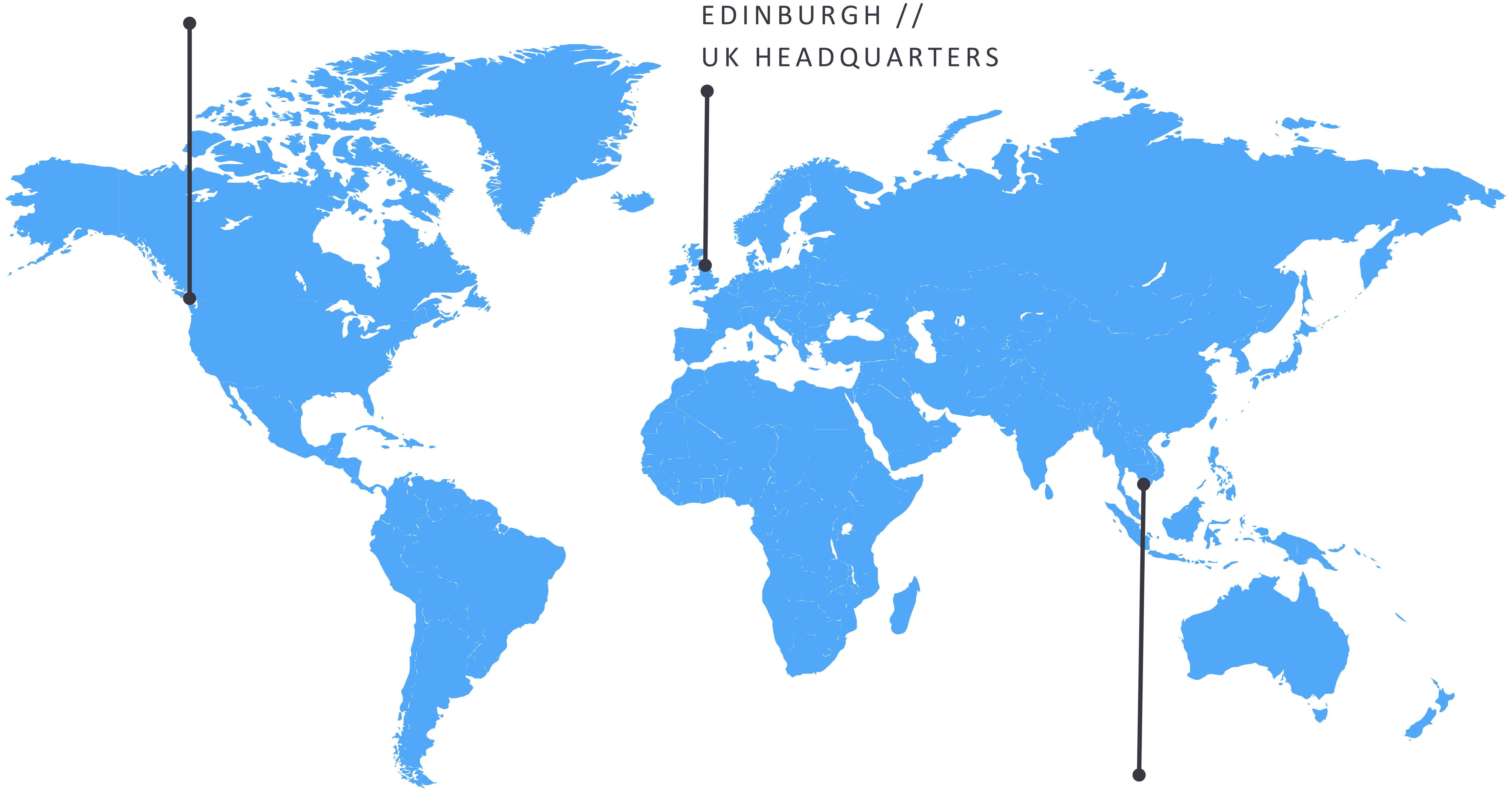
Strategic partnerships with governments, research institutions, professional associations and industry

CSA research is FREE!

2009
CSA FOUNDED

SEATTLE/BELLINGHAM, WA // US HEADQUARTERS

EDINBURGH // UK HEADQUARTERS



SINGAPORE // ASIA PACIFIC HEADQUARTERS

CSA Research Facts

- In 2009 we produced 2 research artifacts
- Since 2010 CSA has produced over 161* Research Artifacts
- We have a total of 34 Research Working Groups (26 Currently Active)
- Over 4500** Volunteers have been involved (Past & Present)

* Does not included some regional research, CCM Mappings Activities, Grant Deliverables, Commissioned Projects, Planned work for 2017 Q1-Q4
** Individuals logged into Basecamp

CSARS Serbian Chapter cloud security alliance®

CSA Serbian chapter

Mission and vision

- Promote cyber security for cloud environments
- Support creation and implementation of cyber security standards
- Development of trust

- Gather experts form different areas
- Establish local cloud security community
- Help local players to promote and establish security culture for cloud environment

CSA Serbian chapter

Members and activities

- Members from different industries
- Variety of expertise and interests
- It is free and worth a lot
- Are you our next member ???

- Define activities for 12 month period
- Make marketing promotions
- Participation in significant security events in Serbia

COME AND JOIN US

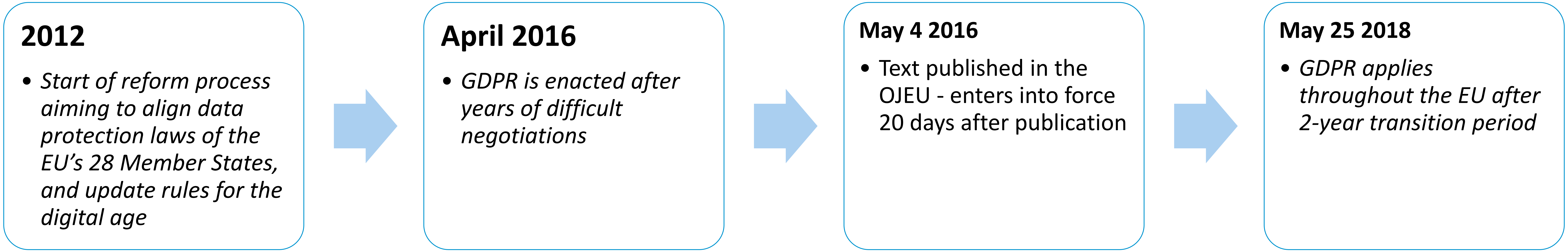
CSA Serbian chapter

Activities

- Localization of valuable content
- Join to major events to promote cloud security
- Work with CSP to increase level of cloud security

MANAGING PERSONAL DATA PROTECTION COMPLIANCE WITH THE GDPR: CSA PRIVACY LEVEL AGREEMENTS (PLA V3 COC) FOR CLOUD SERVICE PROVIDERS

EU Data Protection Reform



2012

- *Start of reform process aiming to align data protection laws of the EU's 28 Member States, and update rules for the digital age*

April 2016

- *GDPR is enacted after years of difficult negotiations*

May 4 2016

- Text published in the OJEU - enters into force 20 days after publication

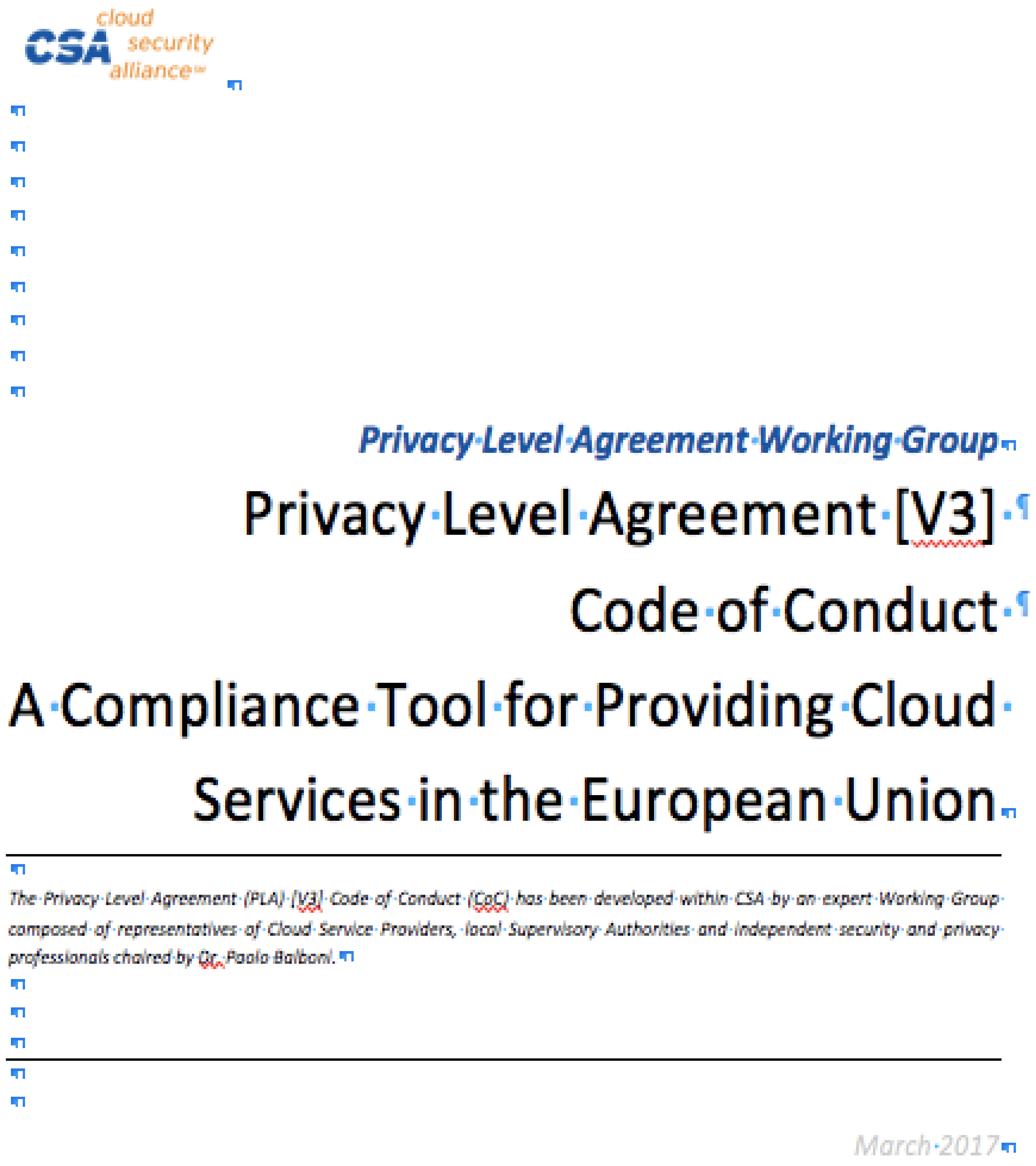
May 25 2018

- *GDPR applies throughout the EU after 2-year transition period*

CURRENT LEGAL FRAMEWORK BASED ON DIRECTIVE 95/46/EC INCONSISTENT PATCHWORK OF NATIONAL LAWS.

GDPR OBJECTIVES: HIGH LEVEL OF PROTECTION (MAINTAINS DATA PROTECTION PRINCIPLES), MODERNIZATION, HARMONIZATION, MORE EFFECTIVE IMPLEMENTATION

CSA Privacy Level Agreement (PLA V3)



Privacy Level Agreement Working Group

Privacy Level Agreement [V3]

Code of Conduct

A Compliance Tool for Providing Cloud Services in the European Union

The Privacy Level Agreement (PLA) [V3] Code of Conduct (CoC) has been developed within CSA by an expert Working Group composed of representatives of Cloud Service Providers, local Supervisory Authorities and independent security and privacy professionals chaired by Dr. Paolo Balboni.

March 2017

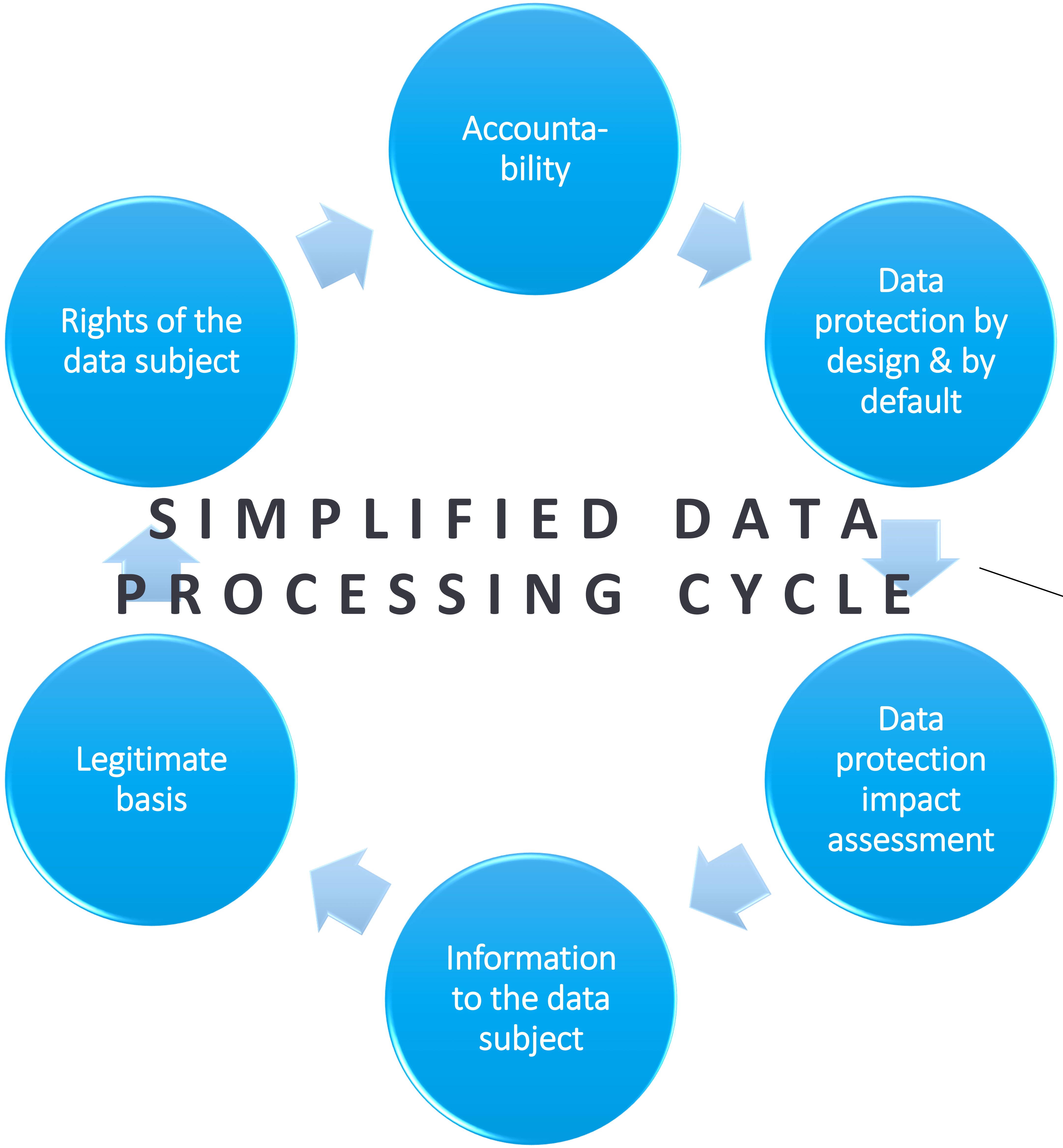
Goal:

- Provide CSPs a tool to achieve EU-wide data protection compliance with the GDPR
- Provide cloud customer with a tool to evaluate CSP EU-wide data protection compliance with the GDPR

Structure:

- Follows EU actual and forthcoming Data Protection Law
- Considers differences between CSP-controller and CSP-processor

SIMPLIFIED DATA PROCESSING CYCLE



Accountability

Data protection by design & by default

Data protection impact assessment

Information to the data subject

Legitimate basis

Rights of the data subject

PLA V3

PLA V2(V3) Table (Annex 1)

	A	B	AD	AE	AF	AG
1			Mandatory under "EU Data Protection Law"	Mandatory under only some of the EU Member State laws		
2					CSP is Data Controller	CSP is Data Processor
3	**1. IDENTITY OF THE CSP (AND OF REPRESENTATIVE IN THE EU AS APPLICABLE), ITS ROLE, AND THE CONTACT INFORMATION FOR THE DATA PROTECTION INQUIRIES**	*Specify:*				
4		*- CSP name, address, and place of establishment;*	Yes		Applicable	Applicable
5		*- Its local representative(s) (e.g. a local representative in the EU);*	Yes		Applicable	Not Applicable
6		*- Its data protection role in the relevant processing (i.e., controller, joint-controller, processor, or subprocessor);*	Yes		Applicable	Applicable
7		*- Contact details which the customer can use to submit personal data protection related inquiries.*	Yes		Applicable	Applicable
8		*- Contact details of the Data Protection Officer or, if there is no DPO, the contact details of the individual in charge of privacy matters to whom the customer may address requests.*		Yes	Applicable	Applicable
9		*- Contact details of the Information Security Officer, if there is no ISO, the contact details of the individual in charge of security matters to whom the customer may address requests.*		Yes	Applicable	Applicable
10						
	2. WAYS IN WHICH THE DATA WILL BE PROCESSED.	*If the CSP is a controller, provide details on (i) the purposes of the processing for which the data are intended and the necessary legal basis to carry out such processing as per Article 7 Directive 95/46/EC; (ii) any further information such as:* *- the recipients or categories of recipients of the data,* *- the obligatory or voluntary nature of providing the requested data,* *- the existence of the right of access to and the right to rectify the data concerning the data subject* *in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject (Art. 10 Directive 95/46/EC). Distinguish activities*			🟦	🟥

PLA CODE OF CONDUCT

- The CSA Privacy Level Agreement Code of Conduct is a code developed by the PLA WG so to provide a tool for both cloud data processor and cloud data controllers to comply with GDPR requirements.
- The PLA CoC is based on the work done by CSA since 2012 with the release of:

✓ PLA V1: A privacy outline for companies selling cloud services in EU

✓ PLA V1 was created to be a “transparency tool”

✓ PLA V2: It evolves V1 so to create a “compliance mechanism”

✓ PLAV2 was aligned with the requirements of the Directive 46/95/EC as well as with the Opinion 05-2012 of the WP29.

PRIVACY LEVEL AGREEMENT V3: REQUIREMENTS (1)

1. Declaration of compliance and accountability
2. CSP relevant contacts and its role
3. Ways in which the data will be processed

a. Personal data location

a. Subcontractors

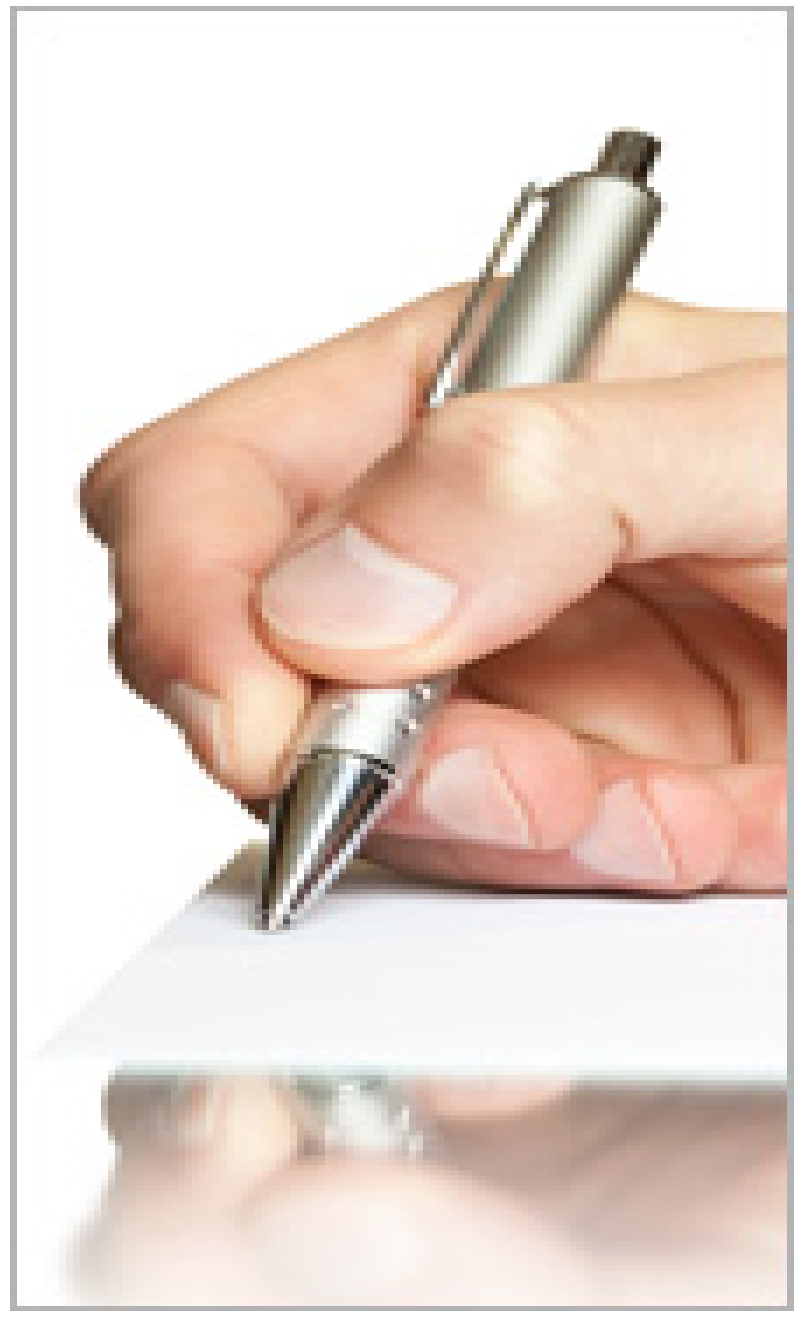
b. Installation of software on cloud customer’s system

c. Data processing contract (or other binding legal act)

4. Record keeping

PRIVACY LEVEL AGREEMENT V3: REQUIREMENTS (2)

5. Data transfer
6. Data security measures
7. Monitoring
8. Personal data breach
9. Data portability, migration, and transfer back
10. Restriction of processing
11. Data retention, restitution, and deletion
12. Cooperation



I think [the PLA Outline] is a very helpful document, both for potential customers of CSPs and for CSPs themselves.

By following closely the WP29 Opinion it ensures that both parties understand the obligations under EU law - probably the strictest requirements they will have to comply with.

Hopefully it will be accepted by CSPs that, if they want to be viewed as acceptable service providers - especially by EU-based organisations - they are going to have to be able to answer successfully the questionnaire that is annexed to the document.

Billy Hawkes,
Irish Data Protection Commissioner

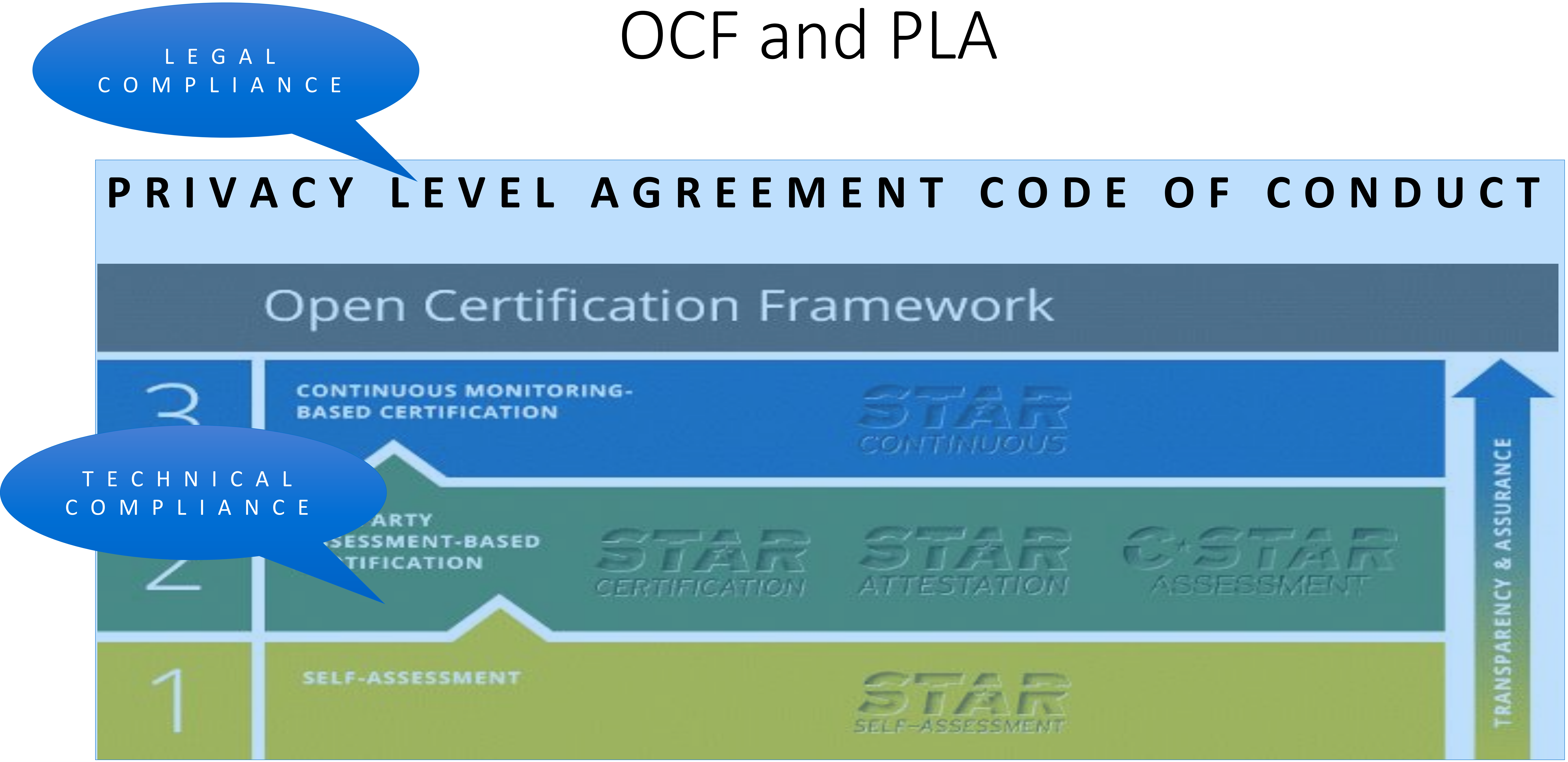
Transparency and information are key to build trust in the cloud ecosystem.

This is why the CNIL has actively contributed to the elaboration of the PLA-outline.

As it gets gradually adopted by CSPs, it will become an important building block for constructing a modern ethical and privacy-preserving framework, adequate to the challenges that face all stakeholders in the digital world.

Isabelle Falque-Pierrotin,
President of the CNIL

OCF and PLA



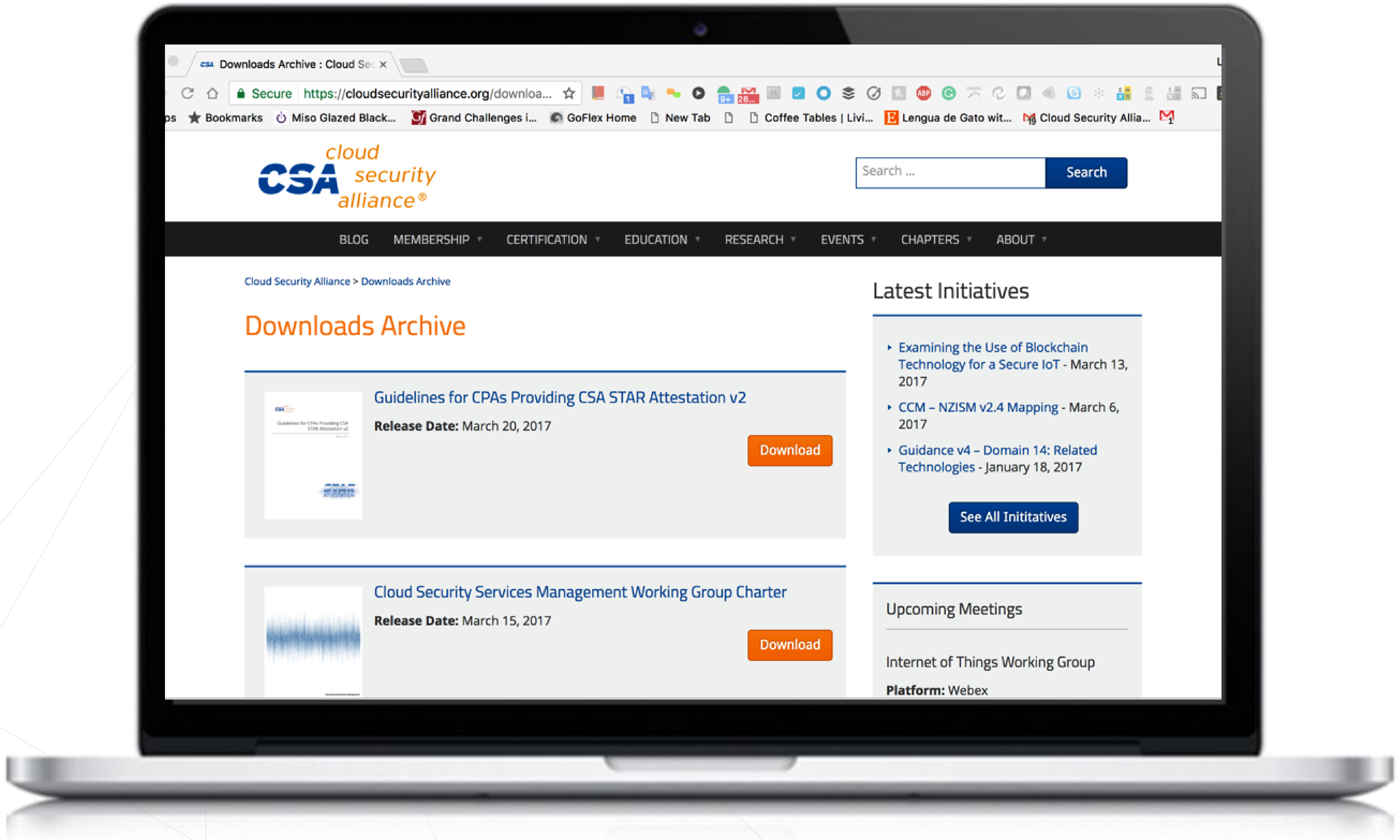
LEGAL COMPLIANCE

PRIVACY LEVEL AGREEMENT CODE OF CONDUCT

TECHNICAL COMPLIANCE

THANK YOU

For that Awesome Presentation



Cloud Security Alliance > Downloads Archive

Downloads Archive

Guidelines for CPAs Providing CSA STAR Attestation v2

Release Date: March 20, 2017

Cloud Security Services Management Working Group Charter

Release Date: March 15, 2017

Latest Initiatives

- Examining the Use of Blockchain Technology for a Secure IoT - March 13, 2017
- CCM – NZISM v2.4 Mapping - March 6, 2017
- Guidance v4 – Domain 14: Related Technologies - January 18, 2017

Upcoming Meetings

Internet of Things Working Group

Platform: Webex

Contact CSA Research

Twitter: @cloudsa

Our Workgroups: www.cloudsecurityalliance.org/research

Learn: www.cloudsecurityalliance.org/research/cloudbytes

Download: www.cloudsecurityalliance.org/download

Resources

https://star.watch/en

https://cloudsecurityalliance.org/star/

https://cloudsecurityalliance.org/group/cloud-controls-matrix/

https://cloudsecurityalliance.org/group/privacy-level-agreement/