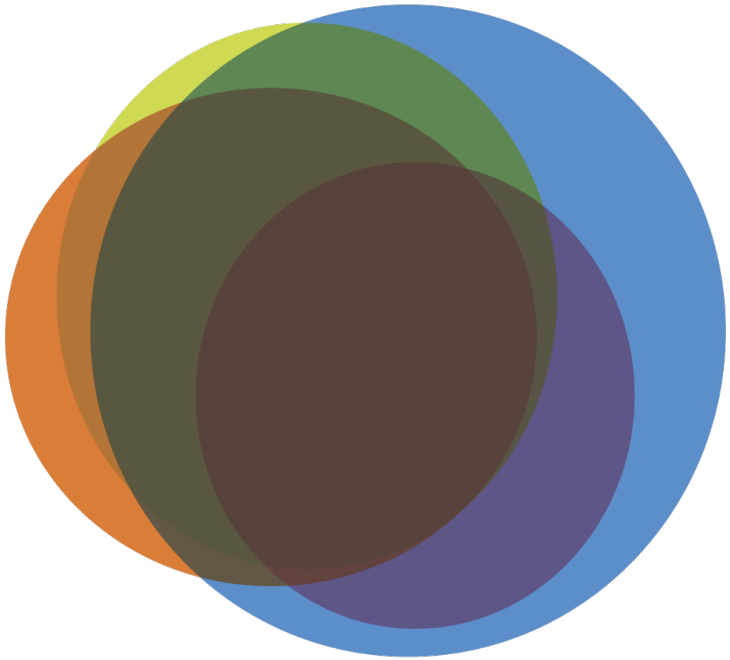


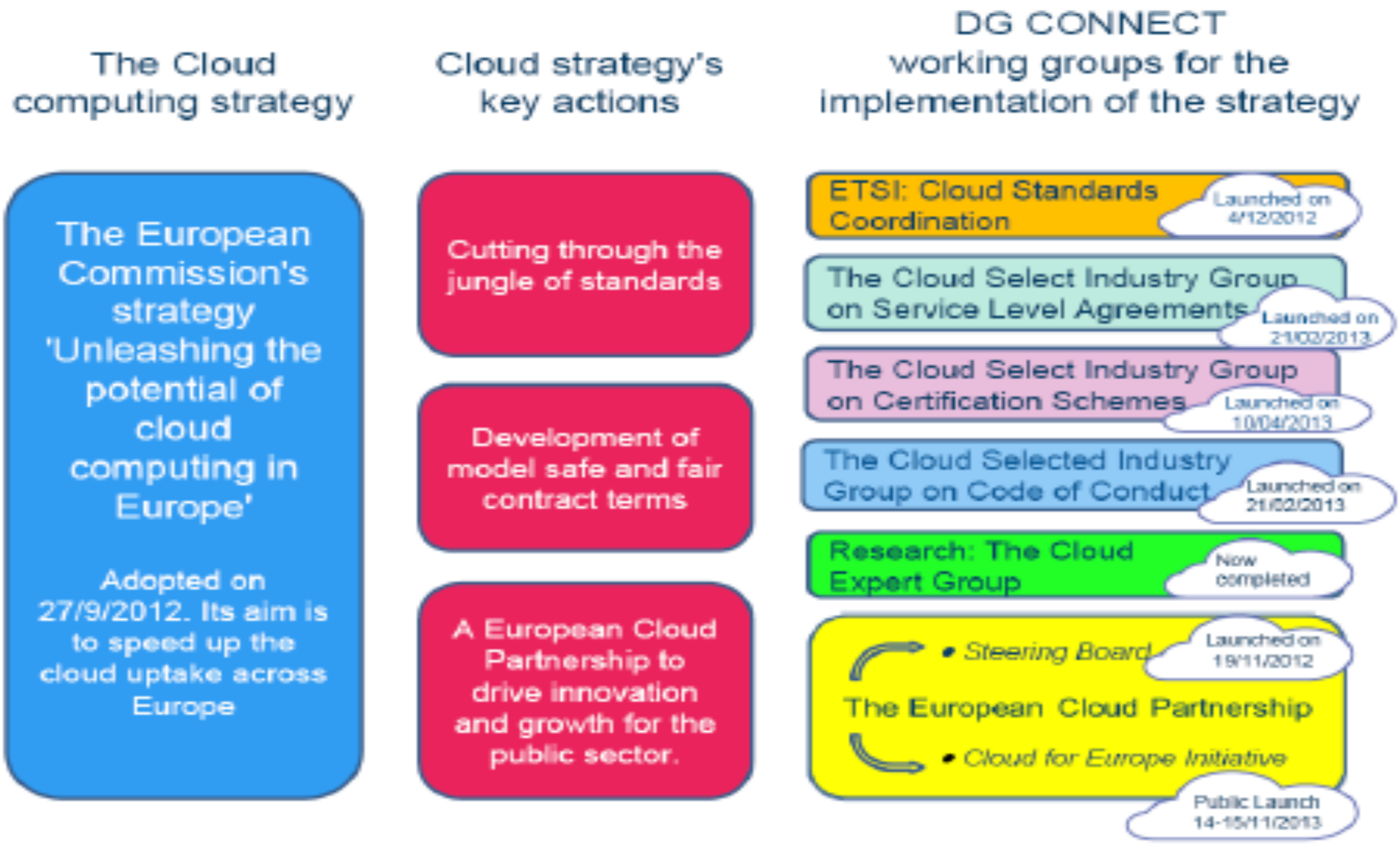
EU Privacy Compliance

CSA PRIVACY LEVEL AGREEMENT and EC CODE of CONDUCT

Daniele Catteddu,
Managing Director EMEA
Cloud Security Alliance

EC C-SIG
Privacy Code of Conduct

EU Cloud Strategy



Privacy CoC: Purpose and Scope

- The Code is a voluntary instrument, allowing a CSP to evaluate and demonstrate its adherence to the Code's requirements.
- The purpose of this Code is to instil trust and confidence among cloud customers that:
  - the personal data to be processed under the CSP Service Agreement (the customer's personal data) are processed with an appropriate level of data protection;
  - an adhering CSP has met the applicable requirements as set out in this Code related to the processing of personal data, in accordance with the EU Data Protection Directive and its national transpositions.
- The Code applies mainly to Data Processors

Conditions of adherence

- (i) self-evaluation and self-declaration of compliance, or
- (ii) by relying on third-party certification.
- Any CSP may sign up to the Code, irrespective of where personal data is stored and processed. CSPs that have demonstrated their adherence to the Code in accordance with its governance processes may use the Code's relevant compliance marks.

Data Protection Requirements

- Contractual specification of the terms and conditions of the CSP's services
- Processing Personal Data lawfully
- Transfer of the customer's personal data within the CSP's Group
- Transfer of the customer's personal data to a subcontractor
- Right to audit
- Liability
- Cooperation with the customer
- Data Subject complaint handling
- Data Protection Authority request handling
- Confidentiality obligations
- Law enforcement/governmental requests
- Data breach
- Termination of the Services Agreement

Security Requirements

- Availability
- Integrity
- Confidentiality
- Transparency
- Isolation
- Accountability

Status

- CoC was sent to Art29 WP on January 2015 for their review and potential endorsement
- Final (?) feedback expected very soon

PRIVACY LEVEL AGREEMENT

Privacy Level Agreement (PLA) v1

- Privacy Level Agreements (PLA) v1 is a powerful **transparency** and **voluntary disclosure mechanism** for those Cloud Service Providers (CSPs) offering services in the European Economic Area (EEA).
- PLA is intended to provide:
  - Cloud customers and potential customers with a tool to assess a CSP's commitment to address information privacy and personal data protection practices (and to support informed decisions); and
  - CSPs with a tool (template) for making privacy and data protection disclosures that address the recommendations and guidance provided throughout 2012 by the Article 29 WP and several EU DPAs.

Content of PLA

1. Contact information
2. Ways in which data will be processed
3. Data transfer
4. Data security measures
5. Monitoring
6. Personal Data Breach Notification
7. Data portability, Migration and Transfer back assistance
8. Data retention, restitution and deletion
9. Accountability
10. Cooperation
11. Law Enforcement Access

DPA's opinions on PLA?

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.

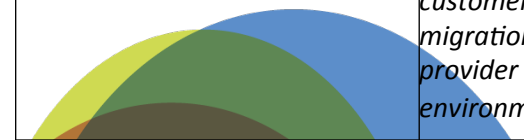
As it gets gradually adopted by CSPs, it will become an important building block for constructing a modern ethical and privacy-preserving framework, adequate to the challenges that face all stakeholders in the digital world.

Isabelle Falque-Pierrotin,
President of the CNIL

Privacy Level Agreement (PLA) v2

- **Objective 1**: Define a PLA Outline for the global market: based on the experience of PLA4EU V.1, the WG will analyze relevant Privacy legislations and define a PLA outline similar to the one defined for the European Union by the PLA WG V.1.
- **Objective 2:** Define a Privacy compliance mechanism for the European Union based on PLA4EU V.1: the Working Group will identify the steps necessary to turn the PLA4EU V.1 from a transparency mechanism into a compliance tool, and to seek for the endorsement of the Art.29 Working Party.

6. PERSONAL DATA BREACH NOTIFICATION A personal data breach is defined by EU Directive 2002/58/EC in Article 2 (i) as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community."	*Specify how, and within what timeframe, customer will be notified of personal data breach affecting CSP and/or its subcontractors*	Yes for electronic communication service providers	Yes	Applicable	Applicable
	Specify how the competent Supervisory Authority(ies) and data subjects will be informed of personal data breaches, and within what timeframe	Yes for electronic communication service providers	Yes	Applicable	Not Applicable
7. DATA PORTABILITY, MIGRATION, AND TRANSFER BACK ASSISTANCE	*Specify the formats, preservation of logical relations, and any costs associated with the portability of data, applications and services*	Yes (This obligation can be inferred from the actual EU data protection legal framework; it is referred to in a number of A29WP Opinions and spcifically set forth in the draft General Data Protection Regulation)	-	Applicable	Applicable
	Describe whether, how, and at what cost CSP will assist customers in the possible migration of the data to another provider or back to an in-house IT environment	Yes (This obligation can be inferred from the actual EU data protection legal framework)	-	Applicable	Applicable



THANK YOU!

CONTACT US

Daniele Catteddu; Managing Director
EMEA, Cloud Security Alliance

dcatteddu@cloudsecurityalliance.org

https://cloudsecurityalliance.org/star/

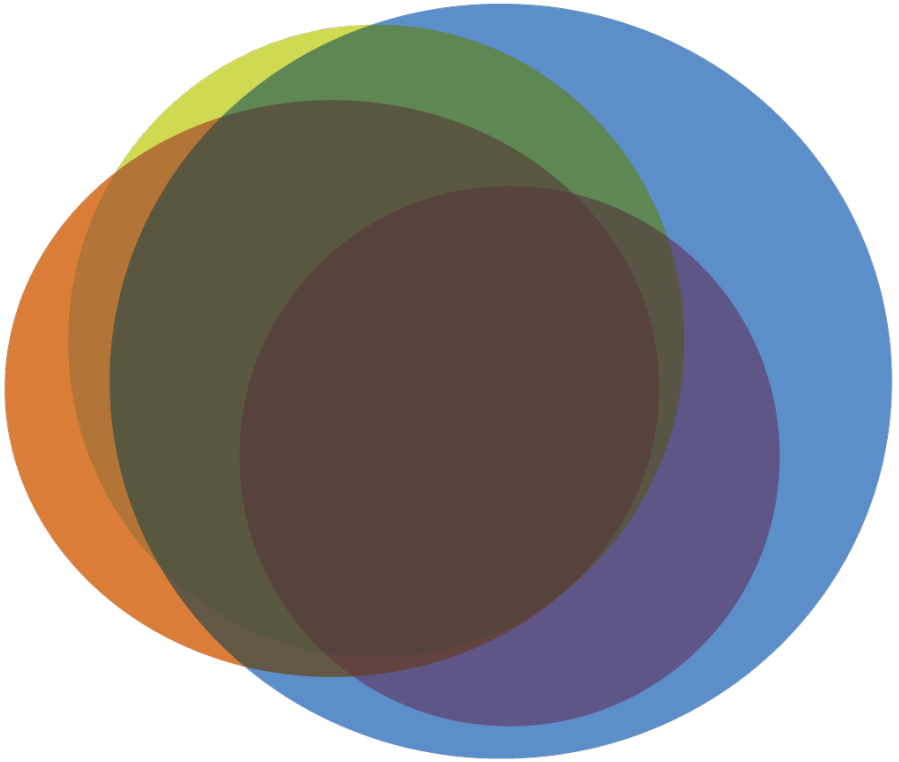
Privacy Contact Person

- Company name, address, place of establishment
- Local representative
- Data protection role in the relevant processing
  - Controller
  - Joint controller
  - Processor
  - Subprocessors
- Contact details of the Data Protection Officer, or privacy contact person to whom customer may address requests

How data will be processed

- Activities performed at the request and on behalf of the customer
  - Organization of data in database
  - Creation of reports
  - Ability to run searches or queries
  - Storage
- Activities performed at the initiative of the CSP
  - Decision to store the data in different countries
  - Decision to implement back-up or disaster recovery centers in different countries
  - Decision to respond to third party request for access

Specific data processing issues



Data location

Use of subcontractors

Installation of software on cloud customer's system

Crossborder data transfers

- Whether the personal data would be transferred, backed-up, recovered, or accessible across borders
- What methods the CSP uses to address the restriction against the transfer of personal data out of the country or region
  - Adequacy decision
  - Model contract clauses
  - Binding corporate rules
  - (Safe Harbor)

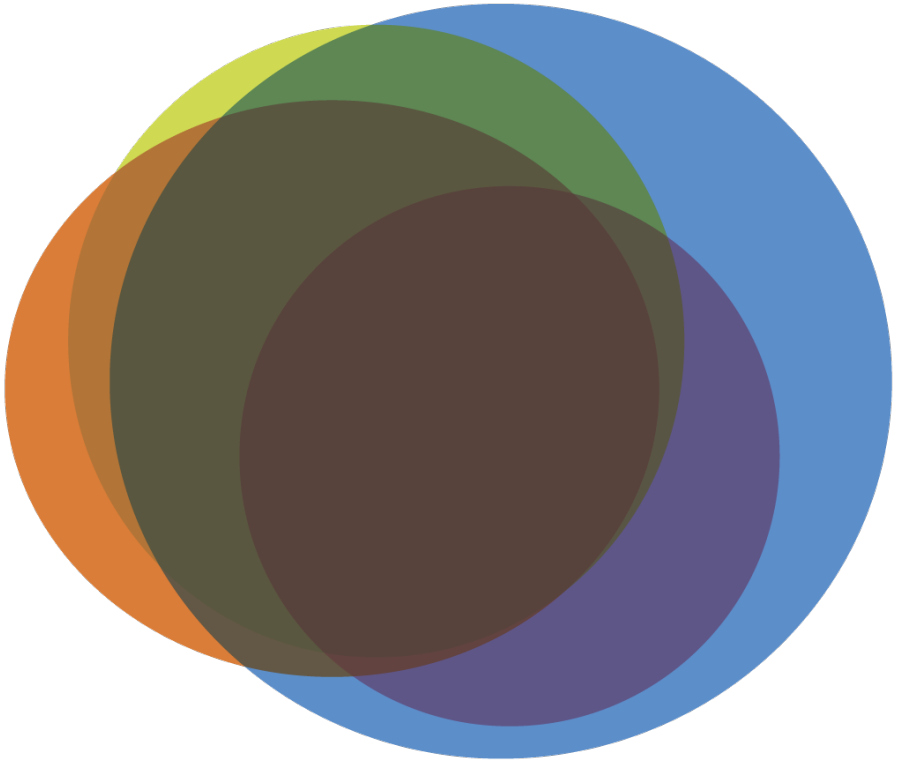
Data security measures

- Identification of the security measures used to protect the personal data
  - Might be a reference to other disclosures regarding the company's information security plan, processes and procedures
  - Might be a description of the security control frameworks followed by the company (e.g. ISO 27002, Enisa Information Assurance Framework, BITS Shared Assessment, CSA Cloud Controls Matrix)
- Customer's ability to monitor / audit the CSP's security practices regarding personal data protection
- Availability of third party audit

Security Breach Disclosure

- Whether the customer will be informed of data security breaches affecting the customer's personal data that occurred on the CSP's network or on the networks of the CSP's service provider, subcontractors, hosting services
  - Within what time frame
  - How

DATA RETENTION, DISPOSAL



DATA PORTABILITY

- Whether and how the CSP will assist the customer in the potential migration of data to another provider

DATA RETENTION

- Duration of data retention

DATA DELETION

- Commitment to delete the personal data in a secure manner