

# Microsoft Cloud Computing Research Centre

5<sup>th</sup> Annual Symposium, September 2018

## Compliance as a Service

Dimitra Kamarinou  
d.kamarinou@qmul.ac.uk

Christopher Millard  
c.millard@qmul.ac.uk

Isabella Oldani  
isabella.oldani@unitn.it

# The brave new world of GDPR compliance

- Under GDPR, a cloud service provider (as processor) and its customer (as controller) have increased compliance obligations and mutual-dependencies
- GDPR compliance requirements are likely to be overwhelming in scale and complexity for many organisations (including, but by no means only, SMEs)
- CSPs are making claims not only about their own GDPR compliance but also how they can facilitate their customers' compliance
- We looked at 13 major CSPs' DP Agreements in the light of Art 28 GDPR and considered the boundaries of the concept of Compliance as a Service



But first...

...what are CSPs promising?

# All AWS Services GDPR ready

by Chad Woolf | on 26 MAR 2018 | in Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Config, Compliance, Security, Identity, & Compliance, Webinars | [Permalink](#) | [Comments](#) | [Share](#)

Today, I'm very pleased to announce that AWS services comply with the General Data Protection Regulation (GDPR). This means that, in addition to benefiting from all of the measures that AWS already takes to maintain services security, customers can deploy AWS services as a key part of their GDPR compliance plans.

This announcement confirms we have completed the entirety of our GDPR service readiness audit, validating that all generally available services and features adhere to the high privacy bar and data protection standards required of data processors by the GDPR. We completed this work two months ahead of the May 25, 2018 enforcement deadline in order to give customers and APN partners an environment in which they can confidently build their own GDPR-compliant products, services, and solutions.

AWS's GDPR service readiness is only part of the story; we are continuing to work alongside our customers and the AWS Partner Network (APN) to help on their journey toward GDPR compliance. Along with this announcement, I'd like to highlight the following examples of ways AWS can help you accelerate your own GDPR compliance efforts.

- ✓ Compliance with security standards
- ✓ Compliance-enabling services
- ✓ Compliant DP Agreement
- ✓ Conformity with a Code of Conduct (CISPE)



Have you accepted our GDPR-updated [Data Processing Amendment](#) for G Suite and [Data Processing and Security Terms](#) for Google Cloud Platform? If not, [read the instructions](#) or watch this [video for G Suite](#) and read the instructions [here for Google Cloud Platform](#).

# Compliance & Certifications

Many GDPR requirements can be mapped to controls in international security and privacy standards and industry frameworks.



## SOC 2

Google Cloud undergoes a regular third-party audit to certify individual products against this standard. Our SOC 2 reports gives you a detailed view of our existing controls over security, availability, processing integrity, and confidentiality or privacy in order to assess Google Cloud as your cloud service provider.



## SOC 3

Google Cloud undergoes a regular third-party audit to certify individual products against the SOC 3 standard. Our SOC 3 report gives you a broad view of our existing controls over security, availability, processing integrity, and confidentiality or privacy, serving as a quick reference guide when starting your GDPR risk assessment of Google Cloud as a data processor.

## GDPR Resource Center

### Overview

[Contracts & Terms](#)

[Compliance](#)

[Relevant Products](#)

### GDPR and Google Cloud



#### CSA STAR

CSA STAR encompasses key principles of transparency, rigorous auditing, and harmonization of standards. CSA STAR allows cloud providers to submit self assessment reports that document compliance to CSA-published best practices. Google's [CSA self assessment](#) can help your assessment of our services, particularly as it relates to Article 28 of the GDPR.



#### ISO 27017

The ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing additional implementation guidance for relevant controls specified in ISO/IEC 27002 and additional controls with implementation guidance that specifically relate to cloud services.



#### ISO 27001

[Google Cloud Platform](#), our [Common Infrastructure](#), and [G Suite](#) are certified as ISO 27001 compliant. ISO/IEC 27001 outlines and provides the requirements for an information security management system, specifying best practices and details a list of security controls concerning the management of information risks.



#### ISO 27018

ISO 27018 relates to the protection of personally identifiable information (PII), dealing with one of the most critical components of the cloud: privacy. This standard is primarily focused on security controls for public-cloud service providers acting as PII processors, building off of existing ISO 27002 controls with specific items for cloud privacy, along with new controls surrounding personal data.

# Safeguard individual privacy with the Microsoft Cloud

Watch the Safeguarding individual privacy rights with the Microsoft Cloud webcast to learn about essential General Data Protection Regulation (GDPR) topics— plus how Microsoft 365 and the Microsoft Cloud help keep your organization compliant.

[Watch the webcast >](#)

[Read the M365 Blog >](#)

[Overview](#)

[Get started](#)

[Solutions](#)

[FAQs](#)

[Resources](#)

## GDPR frequently asked questions

To assist you and your organization in your journey to GDPR, we compiled a list of frequently asked questions.

[Microsoft and the GDPR](#)

[General](#)

[Personal Data](#)

[FastTrack for Microsoft 365](#)

[Expand all](#)

Does Microsoft make commitments to its customers with regard to the GDPR? ▼

Where can I find Microsoft's contractual commitments with regard to the GDPR? ▼

How does Microsoft help me comply? ▲

Microsoft provides tools and documentation to support your GDPR accountability including support for Data Subject Rights, performing your own Data Protection Impact Assessments, and working together to resolve personal data breaches. Visit [Getting Started: Support for GDPR Accountability](#).

# Our commitment to support your GDPR compliance starts right here

## What is the GDPR?

On May 25, 2018, a European privacy law, the General Data Protection Regulation (GDPR), will take effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents.

This site is designed to provide you information about the capabilities in Microsoft services that you can use to address specific requirements of the GDPR. Access the documentation helpful to your GDPR accountability, and to your understanding of the technical and organizational measures Microsoft has taken to support the GDPR. Documentation for Data Protection Impact Assessments, Data Subject Requests (DSRs), and Data Breach Notification is provided to incorporate into your own accountability program in support of the GDPR.

Select a topic below to get started:



## Data Protection I...

How Microsoft helps organizations meet their own DPIA obligations

[LEARN MORE >](#)



## Data Subject Req...

How Microsoft Helps Controllers Address Data Subject Requests Under the GDPR

[LEARN MORE >](#)



## Data Breach Notif...

How Microsoft detects and responds to a breach of personal data and notifies controllers under the GDPR

[LEARN MORE >](#)



## Accountability Re...

A convenient way to access the information you may need to support GDPR when using Microsoft services.


[LEARN MORE >](#)

## Additional Supporting Information

A key part of Microsoft support for your compliance to the GDPR are the commitments we make in our agreements that we make with you as a customer. Not only do we stand behind you with those commitments, the GDPR requires specific issues be addressed in our agreement with you. How Microsoft supports those commitments with specific controls is detailed in the Compliance Manager.

# Accelerate your readiness for GDPR with IBM Cloud

Discover the tools and resources you need to manage compliance with the General Data Protection Regulation while driving innovation

 [Register for Forrester webinar](#)

[Get GDPR ready](#)

**GDPR Readiness**

GDPR Compliance

GDPR Non-Compliance

## Turn GDPR into an advantage

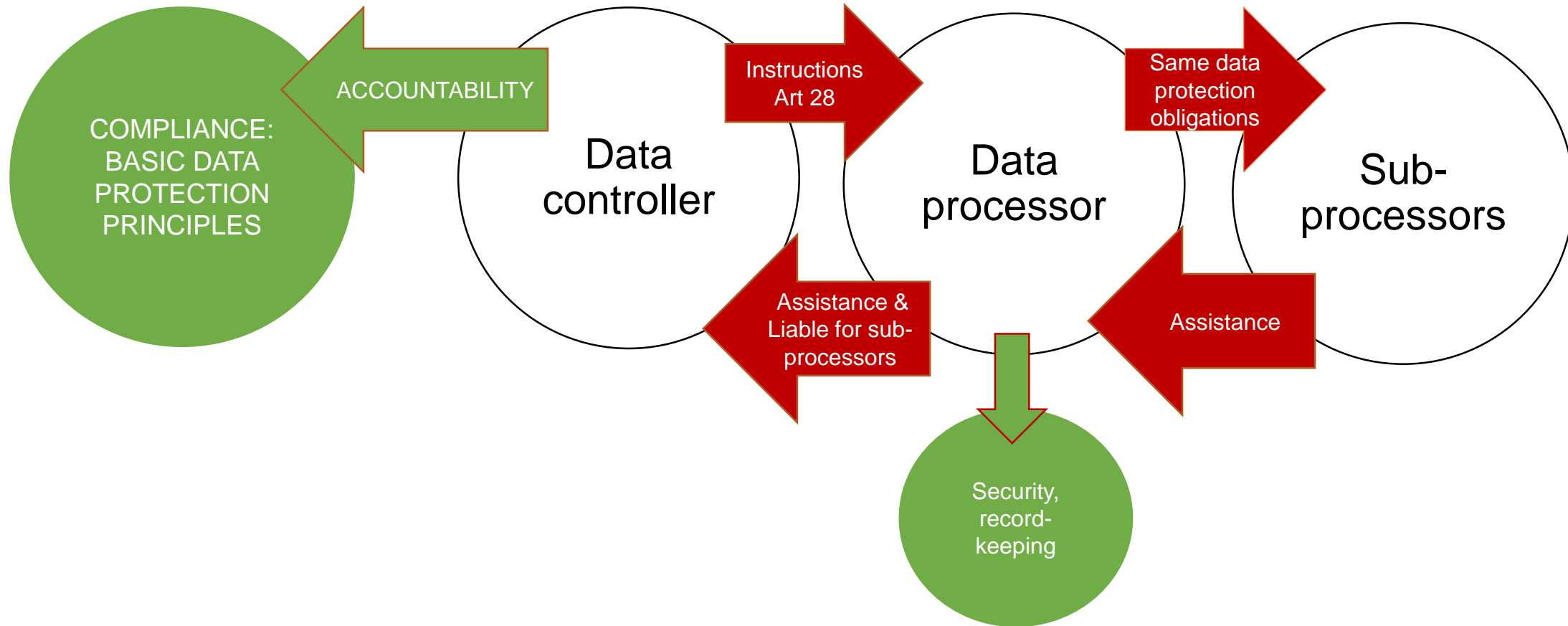
The intent of the General Data Protection Regulation (GDPR) is to elevate protection of the personal data of those in the European Union (EU), regardless of whether your organization has a physical presence there. But rather than merely complying, seize the opportunity presented by GDPR to set your company apart from the competition using the IBM Cloud.

Designed with built-in data security and privacy services, the IBM Cloud offers the platform and tools you need to help safeguard sensitive data wherever it resides. Using IBM data storage and processing products to manage readiness with GDPR, you can gain increased transparency and control over your data, positioning your company to realize efficiencies, identify opportunities and innovate more quickly.

# DP Agreements: themes

1. Relationship between cloud customers & CSPs
2. Security obligations
3. Personal Data Breach Notification
4. Audits
5. Data Subjects' requests
6. Transfers of personal data outside of the EEA

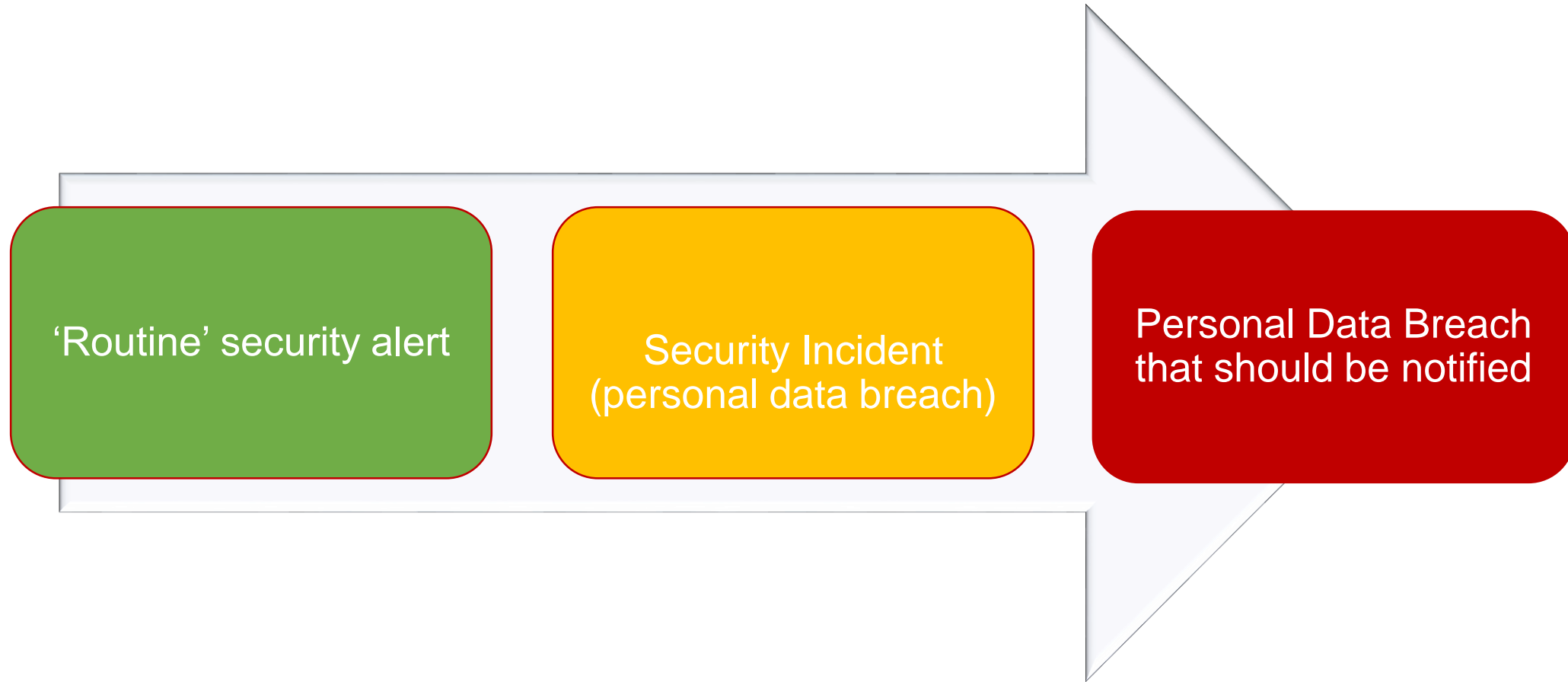
# 1. Cloud customers & CSPs: a symbiotic relationship



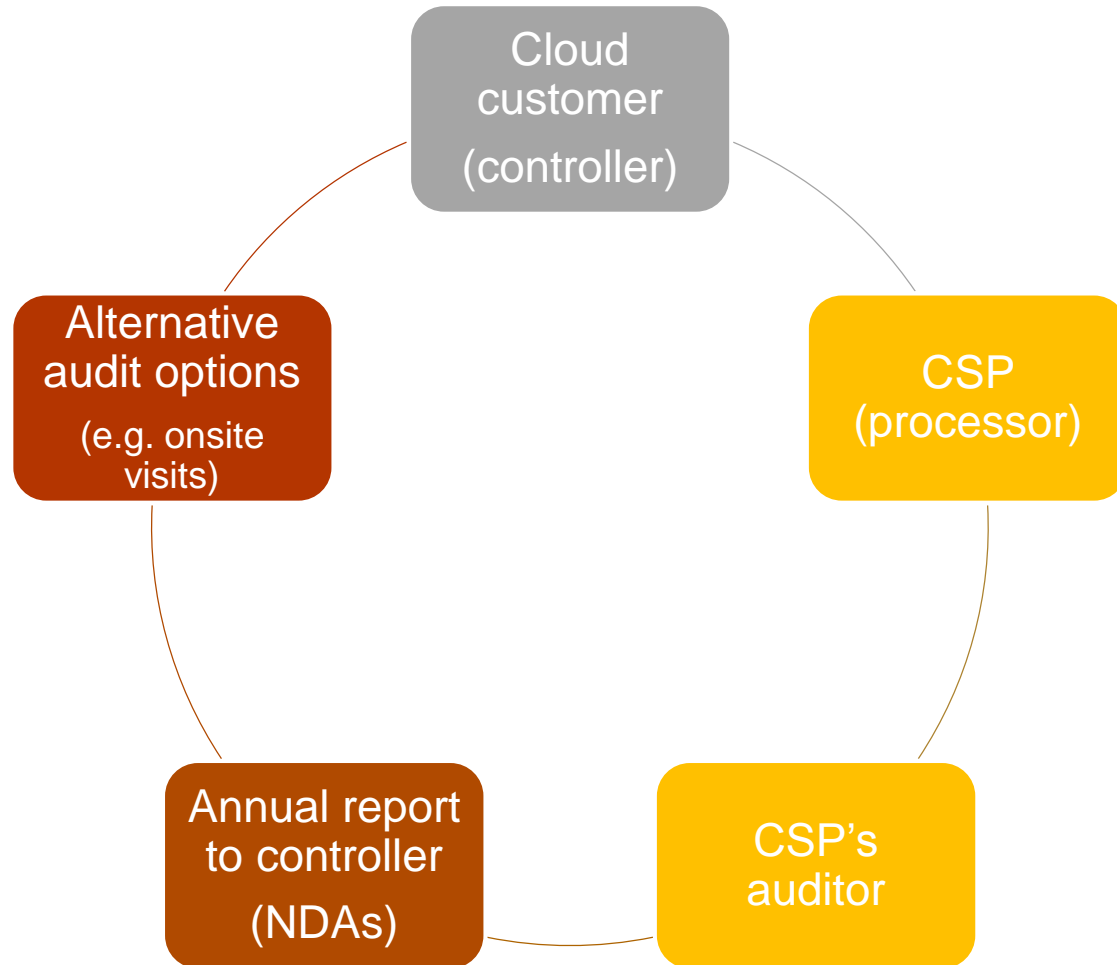
## 2. Security obligations

- Responsibility on both controllers & processors
- ‘Appropriate’ measures
  - state of the art, cost of implementation
  - Article 32
- Assessment of risk:
  - nature of cloud service, scope, context & purposes of processing
  - risk to rights and freedoms of natural persons
- Demonstrating compliance:
  - Codes of conduct (CISPE, EU Cloud, CSA)
  - Certification

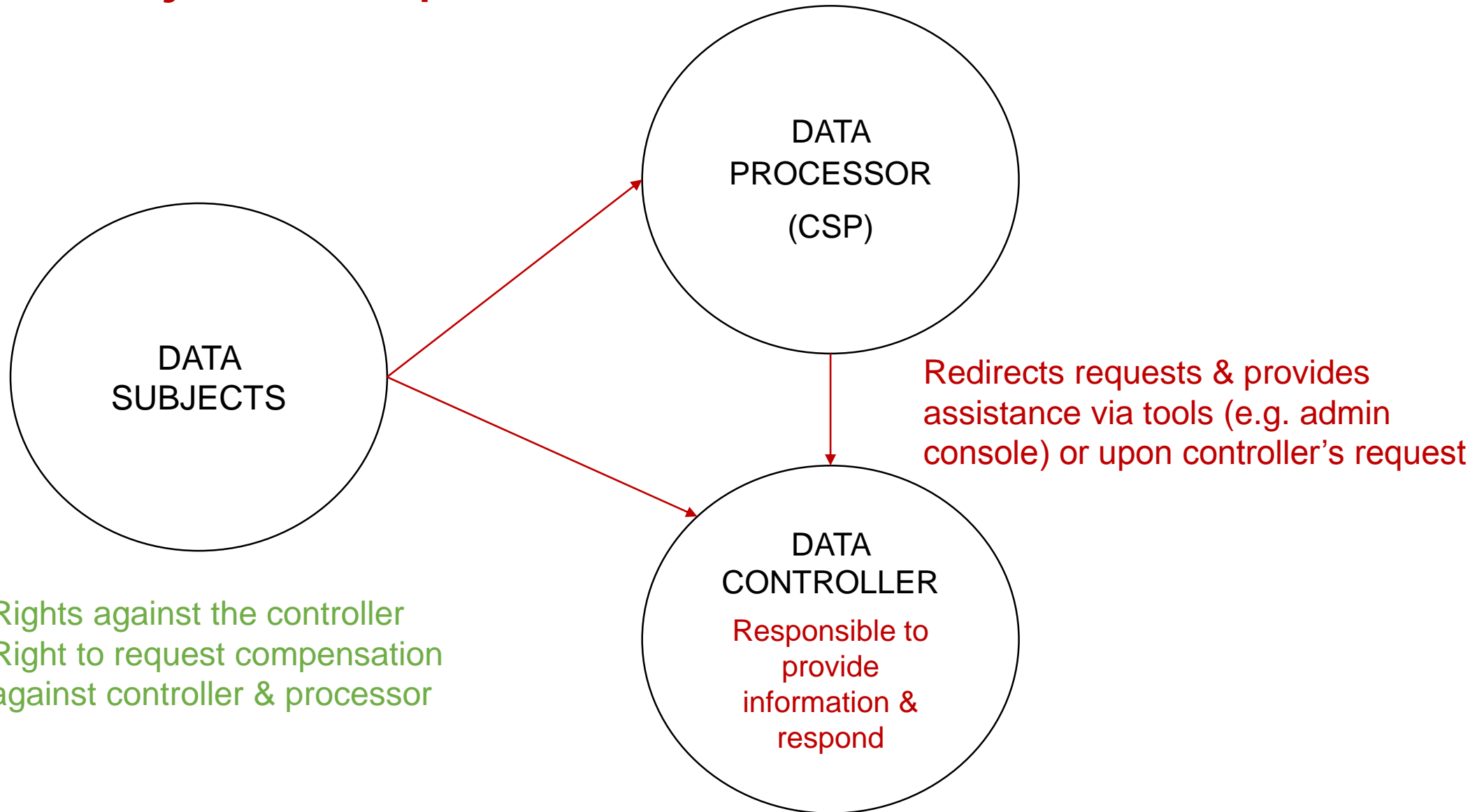
# 3. Personal Data Breach Notification



# 4. Audits

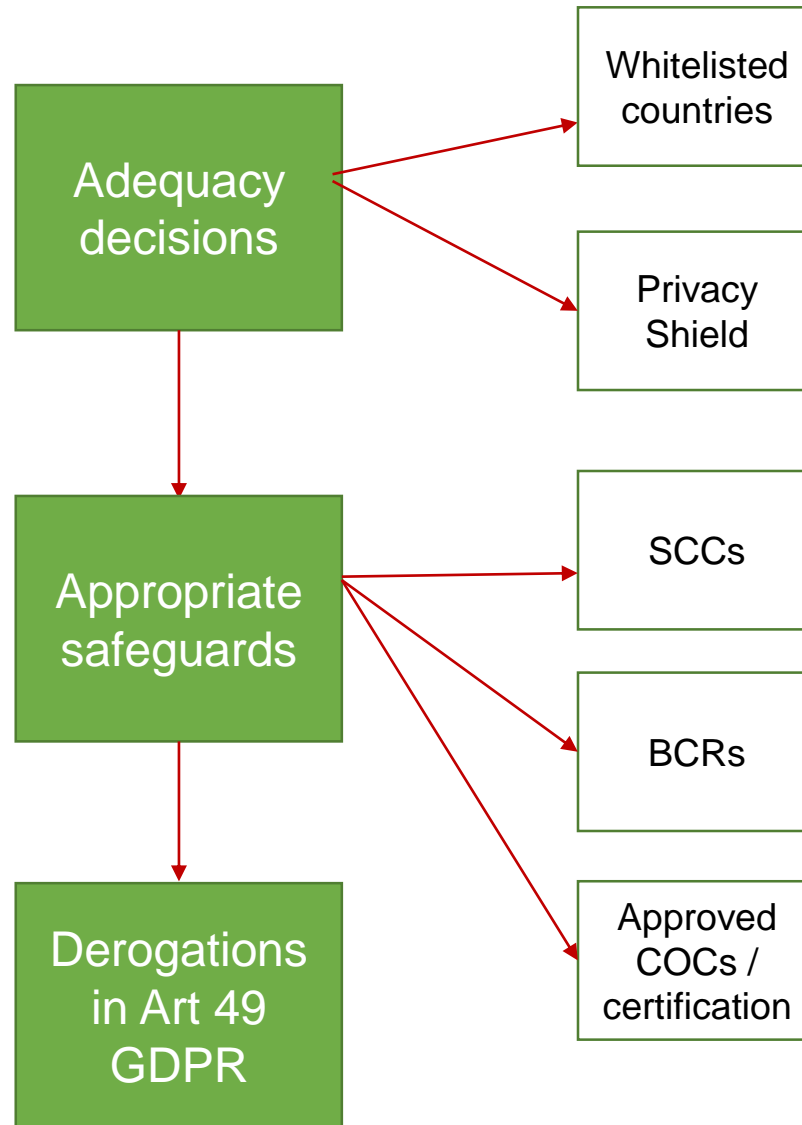


# 5. Data Subjects' requests



- Rights against the controller
- Right to request compensation against controller & processor

# 6. Transfers of personal data outside the EEA



# Transfers of personal data: DP Agreements

- Marketing commitments reflected in DP Agreements
- SCCs & BCRs incorporated in DP Agreements
- Hierarchy of transfer mechanisms
  - BCRs over SCCs and adequacy decisions
  - Why?
- Procedural rules for third parties entering the SCCs
- Data localisation commitments:
  - Customer can choose where data are stored
  - Provider uses only European sub-processors

# Where next for Compliance as a Service?

- What's beyond security commitments, compliance tools and documenting the controller / processor relationship?
- GDPR compliance roles that might be outsourced include:
  - Data Protection Officer
  - EU Representative
- Most CSPs are staying quiet about this, but we did find one CSP that advertises both services...



## Cloud Infrastructure Services

Our public & hybrid cloud platforms come with market-leading performance guarantees and were first to be designed with data privacy & sovereignty at their core.



## Data Privacy Services

Calligo's services instil international, national and industry-specific data privacy requirements into the core of your IT infrastructure and wider processes.



## Data Insights

A portfolio of analytics and artificial intelligence services that help you extract the fullest possible value from your data, underpinned by a 'privacy by design' ethos.

We ensure every data interaction is optimized to deliver maximum business benefit, while meeting all applicable data privacy regulations across all relevant jurisdictions.



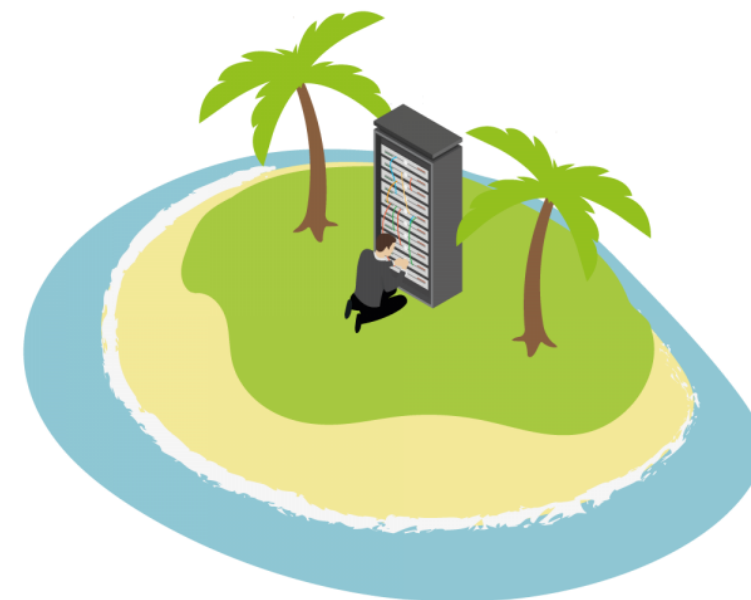


# Forget offshore tax-havens & meet the offshore cloud

## Data privacy, residency and sovereignty

We have developed operational frameworks within CloudCore to assist in the ongoing observance of your data privacy obligations. [Viaje](#), our proprietary cloud management system, features a Policy-Based Engine that allows you to set operational criteria for the use, access and protection of every cloud asset, application and piece of data across your entire environment.

Combining this finite capability with our multi-jurisdictional datacentres, including our provision of Microsoft Azure Stack, we are also able to provide absolute data residency guarantees to our clients.



# Data Protection Officer as a Service (DPOaaS)

[HOME](#) / [SERVICES](#) / [DATA PRIVACY SERVICES](#) / [DATA PROTECTION OFFICER AS A...](#)

If your business is mandated to have a Data Protection Officer, outsource to our data privacy consultants who will monitor your compliance, conduct audits and represent your organisation to data subjects and regulators.

- ✓ Highly skilled consultancy service
- ✓ Experienced in multiple regulatory frameworks
- ✓ Sidesteps the need to hire or internally appoint
- ✓ Balances business objectives and data value with regulatory compliance



# GDPR Services & EU Representatives

[HOME](#) / [SERVICES](#) / [DATA PRIVACY SERVICES](#) / [DATA PRIVACY REGULATION SERVICES](#) / [GDPR SERVICES & EU REPRESENTATIVES](#)

## Outsourced GDPR EU Representative

Organisations who are under the remit of GDPR but do not operate from within the EU are mandated to appoint a representative within the EU to handle their GDPR requests.

Calligo operates in multiple jurisdictions, including the EU, and is able to operate as the appointed GDPR representative for companies outside the EU.



To infinity and beyond...

...the increasingly exotic world of RegTech



## How Blockchain Tech Can Facilitate GDPR Compliance

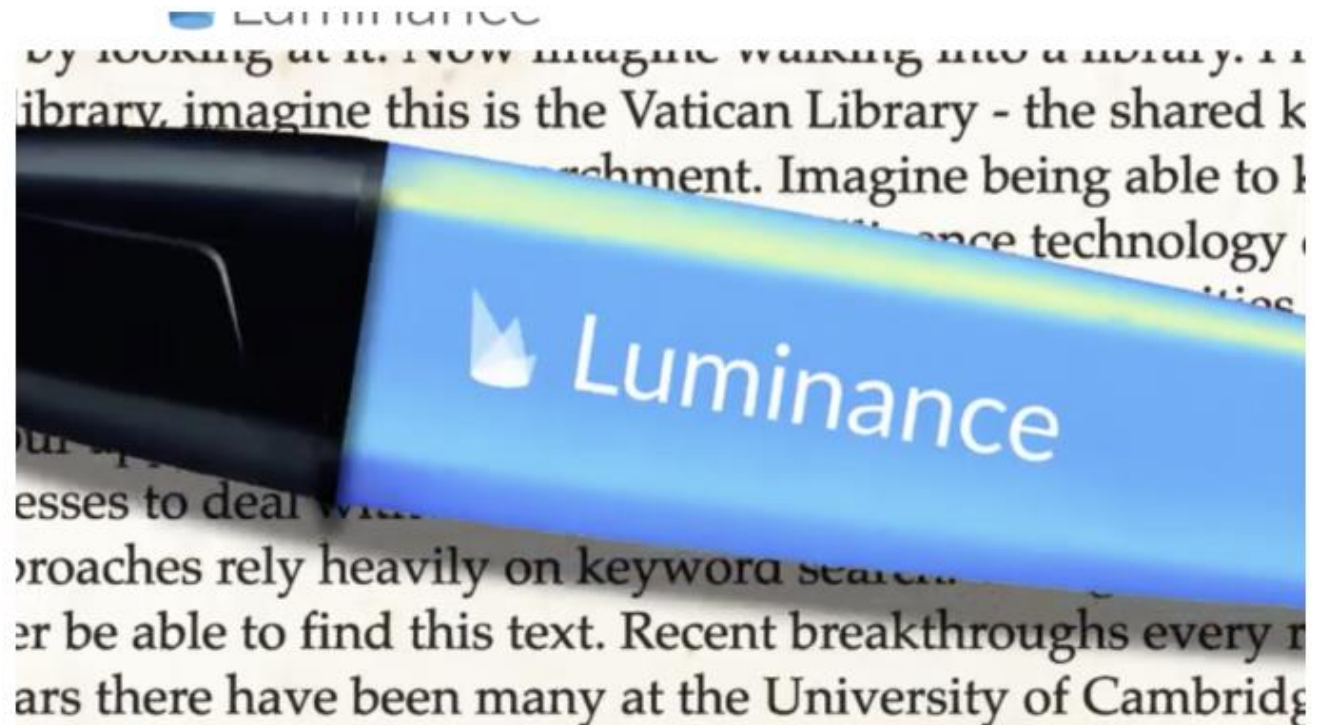
Posted on March 8, 2018 by Armin Ebrahimi 1280



The Role of BYOID in Meeting Requirements

## Legal AI Co. Luminance Now Targets Reg Review, Brexit + GDPR

3rd May 2018 artificiallawyer Legal AI Market Growth 0



Thanks for listening!

*We would welcome comments on our paper...*

*...and are keen to hear about your experiences*