GDPR Compliance: Customer imperatives for choosing the right IaaS provider

Aastha Dhamija

Seattle Pacific University

Abstract

The EU General Data Protection Regulation (GDPR) came into effect on 25th May 2018 and presented one of the greatest compliance challenges faced by global organizations, which became even more complex with introduction of different cloud computing delivery models. While cloud computing came with multiple benefits of greater flexibility and scalability with reduced capital expense, it complicated the application of GDPR's data protection (DP) requirements and their segregation between a cloud service provider (as a data processor) and the organization (as a data controller). These DP responsibilities also vary with different types of cloud computing delivery models i.e. Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). This paper explains this segregation of data processors and data controllers' security responsibilities especially for IaaS providers, with the help of Cloud Infrastructure Service Providers in Europe (CISPE) code of conduct. It also compares leading cloud services providers – Amazon Web Services and Microsoft Azure on those security specific DP requirements and customer imperatives while choosing their preferred cloud partner.

Keywords: GDPR, Data Protection, Cloud Computing, CISPE, SaaS, PaaS, IaaS, Amazon Web Services, Microsoft Azure

GDPR Compliance: Customer imperatives for choosing the right IaaS provider

EU General Data Protection Regulation (GDPR) came into effect on May 25th, 2018 and disrupted the entire data processing regime for all the organizations which were controlling or processing personal data of even a single European resident. This regulation came as a refreshment of former data protection rule of the European region i.e. Data Protection Directive (DPD) that was defined in 1995. It is designed to strengthen the rights of individuals or data subjects regarding the handling of their personal data. And, given the strict penalties (EUR 20 million or 4% of annual worldwide turnover) imposed by this regulation for any kind of data breach, a lot of organizations all over the world are working towards understanding and maintaining compliance with GDPR regulations.

With increasingly sophisticated threat landscape and the colossal amount of personal information many organizations are storing and processing, it is getting extremely challenging to secure every facet of the available information and assure safety of sensitive information of data subjects. And once organizations move from conventional distributed network systems to the cloud environment through Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a service (IaaS) delivery models provided by various Cloud Service Providers (CSP), it becomes even more complicated. There are several reasons for additional complexity as cloud computing introduces the dynamics of multiple players at different locations with multifaceted relationships and disparate vendor (CSP) – customer (organization) security responsibility matrix for each cloud service delivery model (Deyan & Hong, 2012)., as Data Protection (DP) regulations do not apply to all cloud service delivery models in the same manner (CISPE.cloud, 2017). It all depends on the purpose and extent of personal data processing done by the CSP in each cloud delivery model.

One of the major complications which comes with GDPR compliance and cloud computing is difference in responsibilities of the customer organization (as Data Controller) and their CSP (as Data Processors), given that their data can be stored in various parts of the world with a diverse set of other customers in CSP's numerous data centers. Under the GDPR, CSP will have to take some responsibility in the kind of data being processed and how its service, platform, or infrastructure is deployed and utilized by the customer, and hence both customer and CSP are obligated to maintain the compliance as data processors, data controllers or joint controllers and pay potential penalties in case of a data breach, depending on their share of responsibilities. This led to emergence of new code of conducts from various trade bodies and big players in the industry, which defined a set of guidelines for CSPs to comply with the GDPR regulation and made it more transparent for the customers to choose their GDPR compliant data processing partners.

In this paper, we will explore the impact of GDPR on cloud computing, specifically for Infrastructure as a service (IaaS) providers by analyzing different cloud computing code of conducts and how leading CSPs are adhering to those. In section II, we briefly explain the general overview of GDPR, key terms and relevant requirements. In section III, we analyze the impact of GDPR on different cloud computing models, followed by detailed explanation of a specific code of conduct for IaaS providers and minimum DP requirements for GDPR compliance by CSPs (as Data Processors) in section IV. In section V, we take a closer look at security specific DP requirements and responsibility matrix between customer and CSP (only as IaaS provider), followed by explaining how big players like Amazon Web Services (AWS) and Microsoft Azure are complying with those security related technical and organizational compliance requirements section VI. This section also contains a comparison around other

customer imperatives while choosing their preferred CSP data processer, followed by conclusion and ideas for future research in section VII.

The EU General Data Protection Regulation

The first step towards protection of individual's personal data in the EU was the Data Protection Directive (DPD) or Directive 95/46/EC founded in 1995, which outlined the minimum standards for data protection in Europe. Later in 2010, the EU initiated an approach to reform these data protection rules to modernize and align them with the ongoing digital transformation technologies like Big Data, Internet of Things and more. This updated and refined law finally came into existence in 2016 and was adopted as Regulation (EU) 2016/679 or simply the General Data Protection Regulation, abbreviated as GDPR. The main objectives of GDPR as defined in Article 1 of GDPR regulation (GDPR – Official Legal Text, 2019)

- This Regulation protects fundamental rights and freedom of natural persons, particularly protection of their personal data.
- This Regulation lays down rules relating to the free movement of personal data within EU region i.e. movement of personal data from one member state to another, as all EU member states will now follow these minimum DP requirements as a standard.

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (GDPR – Official Legal Text, 2019). It means that this regulation applies to any kind of personal data processing be it manual, automated or being stored in some database as profiling information. And it applies to all controllers or processors who are processing data of EU data subjects irrespective of the location.

As described in Article 4 (GDPR – Official Legal Text, 2019), below mentioned definitions are for the purpose of understanding the GDPR regulation and are also frequently used in this research paper:

- *'**personal data'** means any information relating to an identified or identifiable natural person ('**data subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*
- *'**processing**' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*
- ***'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law, the controller or the specific criteria for its nomination may be provided for by EU or Member State law;*
- ***'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*
- ***'consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear*

affirmative action, signifies agreement to the processing of personal data relating to him or her;

- ***'pseudonymization'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;*
- ***'personal data breach'** means 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;*
- ***'cross-border processing'** means either:*
    - *processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the EU where the controller or processor is established in more than one Member State; or*
    - *processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the EU, but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*

Further, Article 12-23 of GDPR (GDPR – Official Legal Text, 2019) describes the rights of data subjects such as:

- Transparency & Modalities: All rights of data subjects should be concise, transparent, intelligible and easily accessible.

- Information and access to personal data: Data subjects should know the purpose and consent for processing of their personal data , and they should have information and access to services using their personal data i.e. which applications or websites, or any kind of goods/services that are gathering their personal data.
- Rectification and erasure: Data subject have the right to obtain from the controller without undue delay the rectification of their inaccurate personal data or complete erasure of their personal data.
- Right to object: Data subject have the right to object at any time to processing of its personal data for direct marketing.
- Right to data portability: Data subjects can ask controller for an electronic copy of their data and transfer it to another controller.
- Automated individual decision making: Data subjects have the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her.

Article 24-43 of GDPR (GDPR – Official Legal Text, 2019) talks about responsibilities of data controllers and data processors for lawful storing, processing and retention of data subjects' personal information. We will cover these responsibilities in the context of cloud computing and analyze how GDPR DP regulations apply to cloud environment.

From now on, the data controller organization is termed as "customer" and data processing cloud vendor is termed as "Cloud service provider" (CSP).

Impact of GDPR on cloud computing

Cloud computing is the delivery of computing services including servers, storage, databases, networking, software, analytics, and intelligence over the Internet to offer flexible resources and economies of scale without worrying about capital investment and in-house technical expertise. Customers who use cloud computing services for processing of personal data are required to comply with GDPR requirements and their level of adherence is decided by the extent of control over personal information processing i.e. party which decides the purpose and scope of personal data processing. This degree of control varies for the below mentioned cloud service delivery models and ultimately decides their share of responsibilities as per level of adherence:

- **Software as a Service (SaaS):** This represents the most commonly utilized option for cloud services. It utilizes the internet to deliver applications, as majority of SaaS applications run via customer's web browser and are managed by the CSP, a very common example can be Salesforce Customer Relationship Management (CRM). A SaaS CSP has the ability to exercise a wide range of controls in relation to the personal data being processed using its application and is therefore, able to provide technical and contractual commitments to its customers. Hence, CSPs have more degree of control over the kind of data being processed than customers in SaaS model, and are highly responsible for data protection compliance. (Ramgovind et al., 2010)
- **Platform as a Service (PaaS):** PaaS is similar to SaaS, except instead of delivering the software over the internet, PaaS provides a platform for software creation where developers can build or create applications, for e.g. Google Application Platform. Since this platform is delivered via the web, it gives developers the freedom to concentrate on building the software without having to worry about operating systems, updates, storage,

or infrastructure. In terms of access to data, the core application is under the control of developers or the customer, but customer has no direct control over the underlying runtime environment. Hence in this case as well, CSPs have more degree of control than customers but it is less than SaaS model. (Ramgovind et al., 2010)

- **Infrastructure as a Service (IaaS):** IaaS model delivers computing infrastructure, ranging everything from servers, network to operating systems, and storage, all through virtualization, basically allowing customers to purchase resources on-demand and as-needed instead of having to buy the hardware. Unlike SaaS and PaaS, customers have complete flexibility to choose how they want to use that infrastructure, process any kind of data and for whatever purpose. Hence in this case, customers have more degree of control than CSPs over data protection and compliance. (Ramgovind et al., 2010)

For the purpose of this paper, we are going to focus only on IaaS model of CSPs as data processors, and their minimum requirements for GDPR compliance. IaaS model is particularly tricky because of the shared responsibility matrix between the customer and the CSP and even though CSPs don't have much control over the data being processed, they still have to maintain a long list of compliance requirements to facilitate their customers fulfil with the GDPR regulation.

Guidelines for IaaS Cloud Service Providers

GDPR came into force in 2018, however the general discomfort in the cloud industry regarding implications of such a regulation and adoption readiness of various industry players started early. Some bigger players in the cloud industry recognized the importance of this

regulation for continuing their businesses in EU region and also this adoption apprehension amongst organizations, that they started the Cloud Select Industry Group (CISG) in 2012 "to develop the EU Cloud Code of Conduct (CoC) to establish a set of data protection requirements for cloud service providers (CSPs) and support transparent implementation and development of the CoC" (Ceroici et al., 2017). It started as a cooperation between few selected cloud service providers and the European commission, to come up with some industry best practices and a more transparent and definite guideline for CSPs to adhere to GDPR regulations. Founding members of EU CoC included Subject Matter Experts and large Service Providers such as Salesforce, Alibaba Cloud, IBM, Oracle, and SAP (known as Cloud Select Industry Group, CSIG) and an independent body called SCOPE EUROPE was established for overseeing CoC's development and governance rules. This EU CoC was officially launched in 2017 and covered all aspects of cloud services, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

However, given the wide difference between data protection elements and responsibilities of SaaS and PaaS providers versus IaaS providers, few members of the EU CoC felt that these directives were targeted too broadly at Business-to-Business (B2B) cloud services without focusing on the disparities of IaaS providers (Nebuloni, 2017). This led to formulation of a separate code of conduct called Cloud Infrastructure Service Providers in Europe (CISPE), as a spin off from the original EU CoC committee and it extensively focused only on representing IaaS providers as data processers, and their guideline for GDPR compliance.

Table I

Comparison between EU CoC and CISPE Code of Conduct

	EU Cloud Code of Conduct (CoC)	**Cloud Infrastructure Service Providers in Europe (CISPE)**
Scope	Cloud service providers working with all kinds of personal data in the capacity of a processor or controller; for all infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) providers	Only for IaaS Providers; Cloud providers acting only as data processors based on customer instructions
Goals	• To make it easier and more transparent for cloud customers to decide which cloud solutions are the right fit for their needs by providing confidence that member CSPs handle personal data with a level of protection that is compliant with GDPR regulations • To strengthen the confidence in cloud computing by overcoming trust issues between cloud providers and customers	• To eliminate barriers to cloud usage by making it easier for an customer to navigate its GDPR requirements and know if a certain CSP or their hosting service is compliant with GDPR or not. • To help cloud customers in the EU assess if a particular IaaS service provider delivers appropriate safeguards for personal data processing and also support them in maintaining their compliance

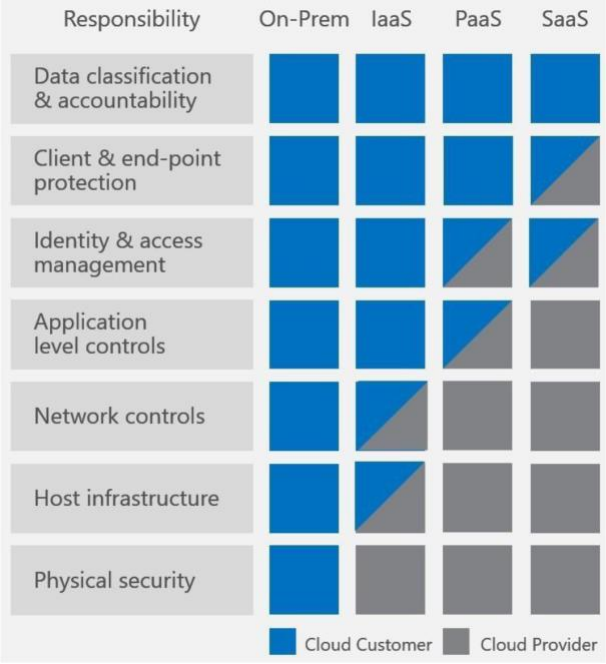
	• To create a future benchmark for secure cloud provisioning in compliance with GDPR regulations	
Compliance Mark	• CoC is not enacted by a public agency, the rules are not enforceable but serve as a strict guide for compliance of member Service Partners.	• Compliance Marks hold no legal value as they are awarded by an industry association without legal powers • CISPE has submitted its Code to the European authorities under Article 27 of the Directive 95/46 and Article 40 of the GDPR. If and when the European authorities recognize that, buyers could refer to the Code adherence as a way to prove GDPR compliance, and even to mitigate penalties in case of a breach.
Adherence	Self-Declaration, Third party audit	Self-Declaration, Third party audit

Essentially both these codes of conducts are trying to help customer organizations find the right fit and GDPR compliant CSPs for their business requirement. In case of SaaS and PaaS cloud delivery models, most of the security requirements are on CSP's side and they are liable to

maintain the compliance, however these responsibilities change in case of IaaS delivery model and that is where CISPE comes into the picture, because it clarifies the security responsibility matrix between customer organization and vendor CSPs. Below is the security responsibility matrix followed by Microsoft Azure for their different cloud delivery models and it clearly shows the differentiation in customer and CSP duties.

Figure I

Shared Responsibility Matrix (Shared Responsibility for Cloud Computing, 2020)



CISPE.cloud (2017) explains this larger difference in case of IaaS delivery model and clearly defines the responsibilities of customer (as data controller) and CSP (as data processor) as per GDPR requirements, which are explained further in the next section.

CISPE Code of Conduct

As mentioned above, this code covers responsibilities of IaaS providers only as data processors and not as data controllers. In this scenario, maximum security responsibilities for lawful processing of personal data falls on the customer rather than CSP and this is the stance which CISPE has taken to further elaborate upon. It focuses on clarifying where the responsibility lies between the customer and IaaS provider or CSP, especially when it comes to security tools and processes. It also encourages a high default level of data protection by CSPs and creates an environment of trust for customers to assess cloud infrastructure services for processing of personal data in compliance with GDPR regulations, and at the same time safeguard small IaaS providers from potential loopholes of joint liability with the customers.

On September 27, 2016, CISPE unveiled publicly in front of the European Parliament and European Commission the first full iteration of the CISPE Data Protection Code of Conduct and after the initial review, the Code was finally signed off by CISPE on January 27, 2017 (Nebuloni, 2017). This code consists of a set of Data Protection (DP) requirements for CSPs as data processors along with their transparency requirements which are essential for maintaining compliance with the code. CSPs can showcase their adherence to the code by either self-assessment or third-party audit and once approved, they get a visual compliance mark in the CISPE public register for their current or potential customers to see. Also, it is important to note that CSPs can have only certain services compliant to the CISPE code and not their entire cloud offering, so customers should be attentive of those and check for all the services mentioned in CISPE public register.

CISPE also contains a governance structure that aims to support the implementation, management and evolution of code for the CSPs. The association of CISPE – comprising of an

Executive board and General assembly are responsible for maintaining this governance structure and updating the code as per evolving privacy regulatory and legislative landscape (CISPE.cloud, 2017). Below are the Data Protection (DP) requirements of CISPE.

DP Requirements

Under CISPE, CSP is just a data processor which provides on demand infrastructure services to the customer (data controller) for processing of any kind of information as per their requirement. Hence in IaaS delivery model, customer is liable for legal obligation of personal data processing, CSP works only as a data processor under the guidance of customer i.e. data controller. The purpose of this section is to clarify CSP's role as a processor under applicable EU GDPR in the context of cloud infrastructure services. The Code of conduct (CISPE.cloud, 2017):

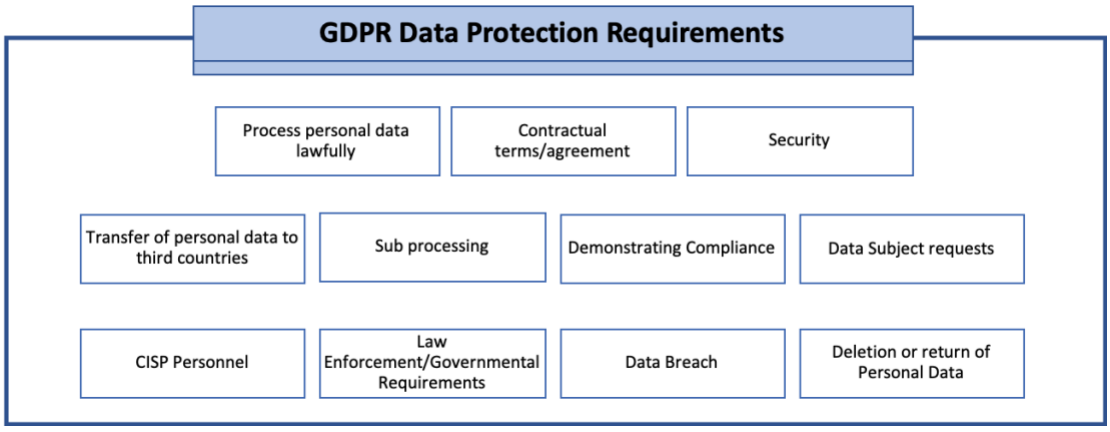
- Identifies DP requirements for processors under applicable EU GDPR
- Applies the identified DP requirement to the cloud services context, and segregates the responsibilities for those requirements between the CSP and the customer
- And further explains how CSP can fulfill their own specific DP requirements and support the customer at the same time

In addition to the code, CSPs are also encouraged to verify all the requirements given under the GDPR law as per their level of exposure to personal data processing. CISPE only serves as a strict guideline for achieving GDPR compliance, as it is still under consideration with European authorities for legal endorsement.

Below showcased diagram covers data protection requirements as mentioned in the GDPR regulation.

Figure II

GDPR Data Protection Requirements



CISPE.cloud (2017) segregates these DP requirements into responsibilities of the IaaS CSP (data processor) and of the customer (data controller) as explained below. Further we provide a note to customer for all the things they should consider while fulfilling each DP requirement.

1. **Processing Personal Data Lawfully**
    a. Data Protection Requirement
        i. *The controller must ensure that personal data is processed lawfully. Processing is lawful only if certain conditions apply. Except where required to comply with law, the processor may process personal data only on documented instructions from the controller* (GDPR Art 28(3)(a)) (GDPR – Official Legal Text, 2019).
    b. Responsibilities of IaaS CSP (Data processor)
        i. The CSP needs to process personal data based on the terms and conditions mentioned in the service agreement contracted by the customer. CSP is only liable to provide all the features and functionalities as requested by the customer, but it is up to the customer to deploy those for lawful

processing of personal data. Hence, CSP's responsibility is limited to (a) complying with the customer's instructions as provided for or reflected in the Service Agreement and (b) providing information about the service in form of regular audits to the customer.

c. Responsibilities of Customer (Data Controller):

   i. Customer needs to define the purpose and scope of personal data processing and ascertain the lawful basis. They need to ensure that the processing is accurate and up to date and only the necessary data is being processed. They are also responsible for safety and confidentiality of personal data and hence need to implement all required organizational and technical controls in partnership with the data processor i.e. CSP.

Note to Customer: In IaaS delivery model, CSP has no control over what information controller/customer chooses to process in their infrastructure and hence have no role either in decision making of what kind of data needs to be processed or defining the lawful basis of the data being processed. It is customer's duty to identify the lawful basis of personal data processing though consent/contract/legal obligation/vital interest/public task/legitimate interest of the data subject and be accountable for processing of that information.

Customer must audit at all the data processing activities being performed by the CSP and verify all required organizational and technical controls in place.

One of the very important requirements of GDPR is to be able to demonstrate compliance, hence customer should maintain an internal document that explains how and why the personal data is being processed.

2. Contractual terms/Agreement

a. Data Protection Requirement:

i. *Processing by a processor shall be governed by a written contract that is binding between the processor and the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The contract may be in electronic form.* (GDPR Art 28(3)). (GDPR – Official Legal Text, 2019).

b. Responsibilities of IaaS CSP (Data processor):

i. The CSP needs to define the features of the service and how it is delivered along with the rights and obligations of the customer in the Service Agreement including (a) Description of processing including compute, storage and content delivery. And, (b) contract, legal terms and conditions and relevant annexures like SLA, service terms, security policies etc.

c. Responsibilities of Customer (Data Controller):

i. Customer need to clearly define the scope of personal data along with the nature and purpose of the processing in the service agreement. They should define the type of personal data, categories of data subjects and duration of the processing. They should verify the duration of data backup and retention policies of the CSP so that the personal information is not kept beyond lawful means.

Note to Customer: As mentioned above, one of the most important requirements of GDPR is to be able to demonstrate compliance, and having a well-defined and clear service agreement is a perfect example of that. A formal contract defines the responsibilities of customer and CSP along with rights and obligations of each. This service agreement forms the basis of all legal compilations of the deal between data controller and processor, hence both the parties need to be extra cautious while executing this document. Customers should especially be thoughtful of all the terms and conditions they put for the processors like scope of processing i.e. limiting the processing to absolute necessary information, defining the exact duration and last day of processing, obligations of each party in case of a breach, frequency of updates from CSP along with the details of dedicated personnel from CSP for continuous monitoring. Basically, every small detail of the deal should be specified in the service agreement and customer should clearly define their own obligations along with expectations from the CSP.

3. **Security**
    a. Data Protection Requirement:
        i. *Both controller and processor must, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk* (GDPR Art 32(1)). (GDPR – Official Legal Text, 2019).
    b. Responsibilities of IaaS CSP (Data processor):

i. The CSP needs to implement and maintain appropriate technical and organizational measures for their data center facilities, servers, networking equipment and host software systems that are within their control and are used to provide the required infrastructure service. Those technical and organizational measures should (1) be designed to help customers secure personal data against unauthorized processing and accidental loss or disclosure, and (2) address the security responsibilities of the CSP

ii. The CSP needs to maintain an Information Security Program to identify reasonably foreseeable risks and minimize them through regular assessments and testing

iii. The CSP needs to conduct periodic evaluation of the effectiveness of above-mentioned security controls and information security program. CSP should also evaluate itself against one or more industry standards.

c. Responsibilities of Customer (Data Controller):

i. The CSP is responsible for the infrastructure it provides, but customer is responsible for all the systems deployed on it, including the security of guest operating systems, applications hosted on the service, data in transit and at rest, customer's service log-in credentials and permissions policies for customer personnel using the service.

ii. Apart from the direct responsibilities, customers should also review the information made available by the CSP relating to data security in respect of the services along with the chosen configuration and features, controls of the cloud infrastructure service in use. They should also verify the

security measures that are under their own sleeve and make an independent determination that together those measures provide an appropriate level of security for the data processing service.

Note to Customer: CSP is responsible for security and compliance of all the infrastructure services it provides to the customer as per the service agreement, but customer itself is responsible for all the systems and applications it deploys on that infrastructure. For example, CSP is responsible for providing multi factor authentication (MFA) as part of its infrastructure security but it is customer's responsibility to make sure that MFA is deployed on all their applications and its employees are using it diligently. Apart from this, customer should also review the security measures implemented by the CSP at their end and determine if they are sufficient for the kind of data being processed. Since it is the customer who decides what data needs to be processed and for what purpose, it is ultimately their responsibility to verify the security measures as CSP does not have any say in monitoring or limiting the scope of processing done by the customer.

4. **Transfer of Personal Data to Third Countries**
    a. Data Protection Requirement:
        i. *Both controller and processor must ensure that any transfer of personal data undergoing processing to a third country shall take place only if certain conditions under applicable EU data protection law are complied with* (GDPR Art 44). (GDPR – Official Legal Text, 2019).
    b. Responsibilities of IaaS CSP (Data processor):

i. Location: CSP need to provide customer the option of storing and processing their data entirely with European region.

ii. Information: CSP need to provide the information about region and country where customer's data is stored, so that customer is aware of the jurisdiction.

iii. Level of protection: CSP need to provide adequate level of protection and provide recognized compliance standard as per EU laws, if data is transferred to another location

c. Responsibilities of Customer (Data Controller):

i. Customer should be aware of the data center location at all times so that they know which EU Member State has jurisdiction over their data

Note to Customer: Wherever possible, customer should always retain their data within European region to avoid additional compliance requirements. Even within EU, customer should keep a tab on the location of data center and double check with their legal team about the personal data processing laws of that particular jurisdiction and if they are fulfilling all the required and lawful obligations. If moving out of EU, then customer should check the treaty of that country around data protection and if that treaty is recognized by

5. Sub Processing

a. Data Protection Requirement:

i. *The processor shall not engage another processor without specific or general written authorization of the controller. In the case of general written authorization, the processor shall inform the controller of the*

intended changes giving the controller the opportunity to object (GDPR Art 28(2)). (GDPR – Official Legal Text, 2019).

ii. *The processor must impose the same obligations as required under applicable EU data protection law in the contract with its controller with its sub-processors. The processor must remain fully responsible to the controller for the performance of their sub-processor's obligations* (GDPR Art 28(4)). (GDPR – Official Legal Text, 2019).

b. Responsibilities of IaaS CSP (Data processor):

i. Consent: CSP needs to take a consent from the customer before introducing a sub processing partner and immediately terminate the contract with sub processor if customer objects. CSP should also mention potential cases and conditions under which it may enlist sub processors in the service agreement itself.

ii. Information: CSP needs to maintain an up to date list of sub processors (along with their location) for accessing customer data, and it should be made available to the customer at the time of service agreement acceptance.

iii. Sub Processing Arrangements: CSP needs to impose equivalent Data Protection contractual obligations to sub processor, to those set out in the service agreement between CSP and customer. CSP will be responsible to maintain and demonstrate compliance as per the service agreement with the customer. And, if sub processors are not processing customers data,

then CSP has no obligation to take consent from customer (like energy suppliers, equipment supplier, hardware vendors etc.)

c. Responsibilities of Customer (Data Controller):

i. Customer should verify all the obligated measures taken by sub processor though appropriate documentary evidence provided by CSP. Customer should be aware of sub processor's data center location at all times to address the EU Member State jurisdiction and should terminate the sub processor's contract at any hint of incompliance.

Note to Customer: Both customer and CSP should always include the clause of sub processors in the service agreement itself, to avoid any kind of discomfort of confusion later on. CSPs will obviously verify all the sub processors under their umbrella as they are directly liable for them, customer should still ask for documentary evidence of all the said security measures and should do periodic audits for compliance.

6. Demonstrating Compliance

a. Data Protection Requirement:

i. *The processor must make available to the controller all information necessary to demonstrate the processor's compliance with its data protection obligations and allow for audits, including inspections, conducted by the controller or an auditor mandated by the controller* (GDPR Art 28(3)(h)). (GDPR – Official Legal Text, 2019).

b. Responsibilities of IaaS CSP (Data processor):

i. Information: CSPs need to make security control information available to the customers so that they can reasonably verify the CSP's compliance with the security obligations in the Service Agreement. Also, there should be a personnel or mechanism for customer to reach to CSP for any kind of information or documentation related to compliance.

ii. Audit: CSP may use independent third-party auditors to verify the adequacy of the security controls applicable to the service. CSP should not allow onsite audits by customer as same location might hold data of different customers and then that would be violation of other customer's security requirements.

c. Responsibilities of Customer (Data Controller):

i. Customer should regularly coordinate with CSP personnel to get all relevant information on security controls in place and check their effectiveness over time through checking audit reports provided by the CSP.

Note to Customer: Since cloud services are multi-tenant environment, customer cannot conduct on site audit as that would be unlawful to other customers' data present in the data center, but they can certainly request for third party audits or audit reports provided by CSP for regular demonstration of compliance.

7. Data Subject Requests

a. Data Protection Requirement:

i. *Taking into account the nature of the processing, the processor must assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising data subject's rights* (GDPR Art 28(3)(e)). (GDPR – Official Legal Text, 2019).

b. Responsibilities of IaaS CSP (Data processor):

i. The CSP should provide the customer with the ability to rectify, erase, restrict or retrieve customer data (a) as part of the service, or (b) by enabling customers to deploy their own solutions using the service. Customer can use this ability to respond to data subjects requests.

c. Responsibilities of Customer (Data Controller):

i. Beyond providing the customer with ability to rectify, erase, restrict or retrieve data, the CSP is not liable for any further assistance with the data subject requests. This is because the customer (and not the CSP) is responsible for managing data subject's processed information using the IaaS service. Hence it is customer's prerogative to accommodate and fulfil data subject's request.

Note to Customer: Customers take consent from data subjects to process their personal information and hence only they are liable to satisfy any of the data subject's request. They can take limited support from CSP to rectify, erase, restrict or retrieve data subject's information but nothing beyond that.

8. CISP Personnel

a. Data Protection Requirement:

i. *Processors must ensure that persons authorized by the processor to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality* (GDPR Art 28(3)(b)). (GDPR – Official Legal Text, 2019).

b. Responsibilities of IaaS CSP (Data processor):

i. Confidentiality: CSP needs to impose appropriate contractual obligations regarding confidentiality on any authorized personnel to access customer data.

ii. Access controls: CSP needs to implement the principle of least privilege when processing customer's data . And when CSP personnel no longer needs to process customer data, then its access rights should be immediately revoked.

c. Responsibilities of Customer (Data Controller):

i. Customer is responsible for maintaining access control of its own employees who are dealing with CSP personnel.

Note to Customer: All CSP personnel working on customer's data processing should be obligated with confidentiality and least privilege. access control. CSP maintains the access control on infrastructure side, but customer needs to maintain the access control for all the systems and applications they deploy on that infrastructure service

9. Law Enforcement/Governmental Requirements

a. Data Protection Requirement:

i. *Processors may only give effect to a court judgment or administrative decision of a third country requiring personal data to be transferred or disclosed if based on an international agreement (e.g. MLAT) between that third country and the EU or a Member State* (GDPR Art 48). (GDPR – Official Legal Text, 2019).

b. Responsibilities of IaaS CISP (Data processor):

i. The CISP will not disclose customer data to a third country law enforcement agency unless it is complied with a valid and legally binding court judgment. CISP will inform the customer before disclosure to provide the customer with the opportunity to seek protection from disclosure.

c. Responsibilities of Customer (Data Controller):

i. Customer should always be aware of the jurisdiction of the particular EU or nor EU member state where its data is being stored and processed by the CSP.

Note to Customer: It is very important for the customer to be aware of data center's location so that they can pre examine the jurisdiction of that member state and are ready in case of any lawful enquiries. Customer should also include this clause of governmental requirements in the service agreement so that they don't miss the chance of seeking protection from unnecessary or unlawful disclosure.

10. Data Breach

a. Data Protection Requirement:

   i. *Processors must notify a data breach to the controller without undue delay after becoming aware of it* (GDPR Art 33(2)). (GDPR – Official Legal Text, 2019).

   ii. *Taking into account the nature of the processing and the information available to the processor, the processor must assist the controller in ensuring compliance with its obligations to notify data breach to the supervisory authority and data subjects* (GDPR Art 28(3)(f)). (GDPR – Official Legal Text, 2019).

b. Responsibilities of IaaS CSP (Data processor):

   i. (a) Security Incident Management Policy: CSP needs to implement a security incident management policy that specifies the procedures for identifying and responding to security incidents, and a description of information to be made available to the customer in case of a data breach.

   ii. (b) Security Notification Breach: The notification will (i) describe the nature of the security breach, (ii) describe the consequences of the breach, (iii) describe the measures taken or proposed by the CSP and (iv) provide a contact point at the CSP. All his should be notified to the customer without any undue delay.

c. Responsibilities of Customer (Data Controller):

i. Customer is responsible for defining the acceptable procedure of identifying and notifying security incident in the service agreement. They are also liable to notify to the data subjects as per the law.

Note to Customer: Customer needs to define the agreeable playbook of data breach identification and notification in case of any security incident. It should provide CSP with a dedicated contact to be notified in case of any security incident and should also maintain a defined playbook at their end to further inform their own data subjects and legal authorities.

11. Deletion or return of personal data

a. Data Protection Requirement:

i. *At the controller's option, the processor must delete or return all personal data to the controller (and delete existing copies) at the end of service provision* (GDPR Art 28(3)(g)). (GDPR – Official Legal Text, 2019).

b. Responsibilities of IaaS CSP (Data processor):

i. Depending of the type of service, the CSP may provide the customer with the ability to retrieve and delete customer data (a) as part of the service, or (b) by enabling customers to design and deploy their own deletion and retrieval solutions using CSP's service.

c. Responsibilities of Customer (Data Controller):

i. It is customer's responsibility to manage deletion and retrieval of data on the Infrastructure service taking into account all the terms and conditions triggered by the termination or expiry of the Service Agreement.

Note to Customer: Customer is in contract with data subjects for processing of their data, hence they are only liable to deletion or retention of that data based on their lawful contract with the data subject. CSP can only support customer by providing them the ability to delete or retrieve data from their data centers.

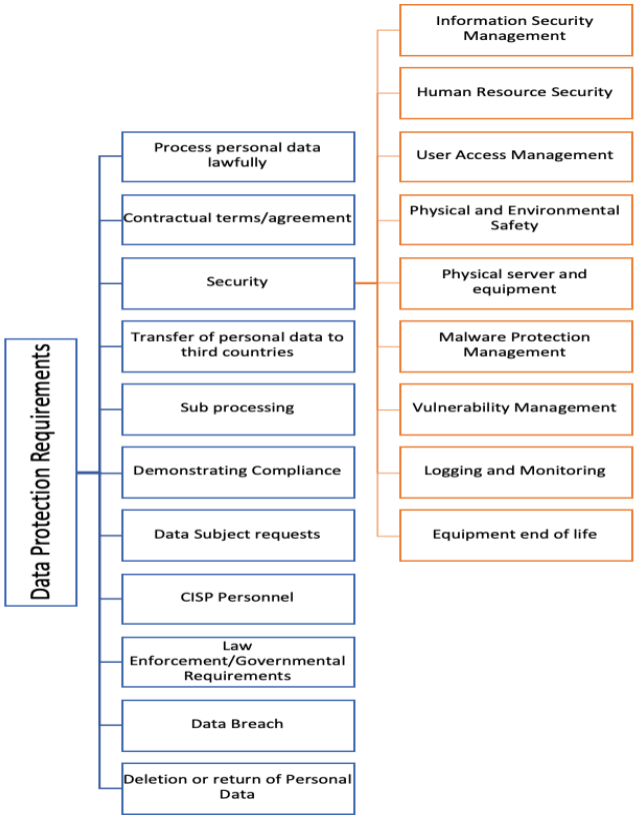
Security requirements of Data Protection Regulations

Out of all DP regulations mentioned in the last section, security is the most demanding and complicated one in terms of number of technical and organizational controls required and their distribution between customer and CSP. Primary objective of these security specific DP regulation is to secure personal data processing and to have required technical and organizational measures in place for protection against unauthorized processing and accidental loss, access or disclosure of information.

The CSP is responsible for security of all the infrastructure services it provides, and customer is responsible for all the systems and applications it deploys on that infrastructure. Below diagram showcases further distribution of security DP regulation into technical and organizational controls which both customer and CSP needs to implement in their respective parts for safer data processing. (CISPE.cloud, 2017)

Figure III

Security Data Protection Requirements



For each of the above mentioned technical and organizational control, we will segregate the responsibilities of customer and CSP, as required under GDPR regulation and guided by CISPE code of conduct. This is defined only in the context of IaaS delivery model with customer as data controller and CSP as data processor. (CISPE.cloud, 2017)

Table II

Security Controls: CSP & Customer responsibilities

Control	CSP Responsibility	Customer Responsibility
Information Security Management	• CSP should have management level direction, support and approved set of security policies to govern the information security management system • CSP should have a designated person to coordinate and be accountable for info security management system	• Customer should designate a point of contact from their side for any kind of security issues • Customer should perform risk assessment to evaluate the suitability of cloud infra service provider based on the privacy regulations.
Human Resource Security	• CSP should have a defined organizational structure for implementation of information security management system with clearly defined roles and responsibilities	• Customer should be responsible for security of its own personnel and any third party who accesses the cloud infrastructure services provided to the customer
User Access Management	• CSP should provide the customer with an access control system for the infrastructure part. It should include role-based access and passwords, or another	• Customer is responsible for the use and configuration of those access control management systems provided by the CSP. The customer shall be responsible

	authentication policy means. CSP is responsible only for managing access of infrastructure part and not of applications or systems deployed on top of it.	for assigning access rights to the appropriate personnel. • Customer is responsible for access solutions to the systems and applications deployed by the customer on the cloud infrastructure service.
Physical and Environmental Safety	• CSP should implement and maintain physical and environmental security measures for the cloud infrastructure service, like data center building safety, video monitoring, network safety, electricity back up, Intrusion detection etc. Basically, securing the data center where all information is stored and processed.	• Review the information made available by the CSP relating to physical and environmental aspect of data center security • Review their chosen configuration and its related features and controls • Review the security measures that they will put in place themselves and make an independent decision that together those measures provide an appropriate level of security for the kind of processing they wish to perform

Physical Server and Equipment	• The CSP is only responsible for the deployment, operation, configuration and security of all physical hardware equipment included in cloud infrastructure service.	• Customer is only responsible for managing the appropriate configuration of all systems and applications deployed on that cloud infrastructure service.
Malware Protection Management	• CSP should implement malware protection on commonly affected or targeted systems of the cloud infrastructure service.	• Customer is responsible for malware protection management on all the deployed systems and applications on that cloud infrastructure service.
Vulnerability Management	• CSP is solely responsible for vulnerability management of the cloud infrastructure service. It will define distribution of tasks like acceptable delay in deploying patches in infrastructure etc.	• Customer is responsible for vulnerability management on all the deployed systems and applications on that cloud infrastructure service. For example; deploying patches in individual applications and systems on the provided Infrastructure.
Logging and Monitoring	• CSP should provide the customer with monitoring and logging tools for the cloud	• Customer is responsible for the use and configuration of those

	infrastructure service. For example: user access logs, API reporting etc.	monitoring and logging tools provided by the CSP.
Equipment end of life	• CSP should conduct a storage media decommissioning process in accordance with industry standards to make sure no customer data can be retrieved from disposed equipment's storage media.	• Customer should review the information made available by the CSP regarding storage media decommissioning and evaluate if it meets their requirement of lawful processing under GDPR • Customer should also consider the impact of its chosen service configuration along with its features and controls on the decommissioning process.

Hence for most of the security controls, CSP is responsible for implementing those technical and organizational controls at infrastructure level and can support customer in implementing those controls at their system and application level, which are deployed on CSP's infrastructure service. Customer is solely responsible for security at system and application level, CSP can merely provide those tools and services but it is customers prerogative to implement and use them at their end.

Security Requirements in Comparison: Amazon Web Services (AWS) and Microsoft Azure

Big industry players from all over the world (both from EU and non-EU region) like Amazon Web Services, Microsoft, Google, IBM, Oracle etc. are providing cloud infrastructure services in IaaS delivery model and have defined policies and programs to support their customers to comply with GDPR. Top 2 IaaS providers (based on the market cap) Amazon Web Services (AWS) and Microsoft Azure (Azure) are compared below on these organizational and technical security controls under DP regulation.

The comparison is based on CSP responsibilities on these security regulations as mentioned in the CISPE code of conduct and explained in above section. Amazon Web Services (2019) and Microsoft (2019) are the source of this comparison.

From now on, Amazon Web Services is termed as "AWS" and Microsoft Azure is termed as "Azure" in rest of the paper.

- **Information Security Management**
    - AWS: As stated in the service agreement (Amazon Web Services, 2019), AWS maintains a dedicated Information security management program covering both network security and physical security and performs continuous evaluations to support evolving privacy regulatory and legislative landscape
    - Azure: Microsoft Azure maintains a dedicated Information security management program to cover both security and organizational controls required for GDPR compliance. They also have a Data Protection Officer (DPO) to assess risks related to data processing.

Note to Customer: Both organizations claim to have all their cloud services as GDPR compliant and have defined policies and processes in place. AWS is compliant to CISPE code of conduct specifically, whereas Azure follows all GDPR compliance regulations without confirming to any particular code of conduct. Also, both the organizations mention their shared responsibility model with up front customer responsibilities right at the start thereby leaving no scope for confusion.

- **Human Resource Security**
    - AWS: AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.
    - Azure: Azure engineers do not have default access to cloud customer data and are granted access under management oversight and only when necessary. They have limited access policies for their own employees along with the sub-contractors, but the customer can access its own data at any time and for any reason.

Note to Customer: Both organizations have strict policies around customer data access for their own employees as well as sub-contractors, and maintain least privilege and timed access through out.

- **User Access Management**
    - AWS:
        - Customer can define users and roles using Amazon's *Identity and Access Management (IAM) Web service* to securely control access to AWS resources.
        - With IAM roles, customers can allow users to leverage temporary credentials for role session using *Amazon Security Token Service* (AWS STS), which can be used for a defined duration and are generated dynamically, and hence not stored with user account.
        - Customer can also enable Multi factor authentication (MFA) on their AWS accounts
        - To implement granular access to AWS objects, customer can grant different levels of permissions to different people for different resources.
        - Customer can use *AWS systems manager* to see and manage operations of AWS infrastructure and can use AWS *Secrets Manager* service which enables them to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle
        - Customers can use Geo restrictions or geo blocking to prevent users in specific geographic locations from accessing content thru Amazon *CloudFront* (content delivery network) web distribution. They can restrict access at a granular level as well rather than restricting the whole country.
        - Customers can use Amazon *Cognito*, which is product for creating user login and access control features in their web applications and mobile

apps. They can further add MFA or adaptive authentication as per their requirements.

- Azure:
  - Customer can use Azure *Active Directory* (AD) and Azure *Role-Based Access Control* (RBAC) to enforce separation of duties. Both these Azure services are used for secure access control and enable customers to define fine-grained access permissions to grant the minimum level of access that users need to perform their jobs.
  - Customer can use Azure *Key Vault* (tool for securely storing and accessing secrets) for web applications to support separation of duties. This service allows them to implement a segregation of role functionality in the management of keys and data.
  - Customers can use Azure *Active Directory Privileged Identity Management*, this functionality allows them to discover, restrict, and monitor privileged identities and their access to resources. They can also enforce on-demand, just-in-time administrative access when needed.
  - Azure AD also supports identity and access management for virtual machines but must be configured at the virtual machine level.

Note to Customer: Both these organizations provide granular level of access control mechanisms for their customers. They are required to maintain access control only at infrastructure level but provide these extra access control tools and services for their customers to implement at systems and application level. Most of the access control services of Microsoft are connected to their Active Directory, which acts as a universal truth for all their access control functionalities, customers can even implement them even at virtual machine levels. AWS offers different tools like Amazon IAM or Amazon Cognito for different platforms, but they all can be managed together by AWS systems manager. AWS offers more granular level of access control with different tools for each platform whereas Azure links it all to one single source of truth i.e. Azure Active Directory.

- **Physical and Environmental Safety**
  - AWS:
    - All access points are maintained in a secured (locked) state and are monitored by video surveillance cameras designed to record all individuals accessing the Facilities.
    - They also maintain electronic intrusion detection systems to detect unauthorized access to the Facilities, including monitoring points of vulnerability with door contacts, glass breakage devices, interior motion-detection, or other security alert devices for physical safety.
    - All facility entries by employees and contractors are logged and routinely audited.
  - Azure:

- 24-hour restricted access with multiple authentication processes (such as badges, smart cards, and biometric scanners)
- On-premises security guards and monitoring using video surveillance, motion sensors, and security breach alarms along with automated fire prevention and extinguishing systems
- Network for the facilities are secured by restrictive firewall rules and host-based firewall rules along with IPsec policies on hosts and network segmentation to provide physical separation of backend servers and storage devices

Note to Customer: Both AWS and Azure put a lot of focus in choosing the right location for their data centers, depending on the environmental aspects, weather conditions, seismic activity and much more. They both provide 24*7 availability and surveillance with multiple intrusion detection systems and logged entries. Both organizations have also sufficient network security (with firewalls) and redundancy built in for 24*7 availability in case of an incident as well.

- **Physical server and equipment**
  - AWS: All assets are centrally managed through an inventory management system that stores and tracks all necessary information like owner, location, status, maintenance etc. Following procurement, assets are scanned and tracked regularly, and assets undergoing maintenance are evaluated and tracked for ownership and status.

- Azure: Every asset in Azure is given an asset ID which is used to track its complete life cycle in the Azure environment, all from procurement to decommissioning.

Note to Customer: Both the organizations have processes in place for physical inventory tracking at all life stages from procurement to decommission of the assets. It also includes regular maintenance updates and revised ownership details at all times.

- **Malware Protection Management & Vulnerability Management**
  - AWS: SaaS solutions developed by AWS and its partner network can be utilized by customer to take care of this. For e.g. Amazon *GuardDuty* is a threat detection service which continuously monitors for any kind of malicious activity and unauthorized behavior on any kind of data stored in Amazon S3. Customers can also use Amazon *Inspector*, which is a security vulnerability assessment service that helps improve the security and compliance of applications deployed on Amazon EC2. It automatically assesses applications for vulnerabilities or deviations from best practices, and then produces a detailed list of security findings prioritized by level of severity. Such tools or other similar ones can be easily integrated with Amazon Management console (single source to manage all IaaS products and services provided by AWS) for aggregated visibility and control. Though it is provided by AWS, it is customer's duty to install and use them on their own applications and systems.

- Azure: Customers can use *Microsoft Antimalware* for Azure that helps identify and remove viruses, spyware, and other malicious software in real time. It creates alerts when some known malicious software tries to install or run itself on the infrastructure. Customers can also enable *Azure Security Center's* built in vulnerability assessment solution which automatically scans for all kinds of vulnerabilities in the system and report it all back to the security center. Both these solutions are built for applications and multi-tenant environment, but customer needs to implement or enable them themselves based on the needs of application workloads.

Note to Customer: As per CISPE responsibility matrix (CISPE.cloud, 2017), malware protection management and vulnerability on the application and systems deployed on cloud infrastructure services are customer's prerogative and not CSP's. Both AWS and Microsoft offers solutions for Malware management and vulnerability management for their own infrastructure service and those can be extended well enough to customer's applications and systems side, but it is ultimately customers responsibility to enable and maintain them. AWS is more favored with open source community, hence have a good collection of open source Malware protection and vulnerability management tools as well. Unlike Azure, which is majorly partnered only with big names like McAfee, Symantec, Kaspersky etc.

- **Logging and Monitoring**
  - AWS:
    - Customer can use *AWS config* (AWS service to assess, audit and evaluate configurations of AWS resources) to monitor and have a detailed view of

configuration of various resources in their AWS account and how these configurations and relationships change over time

- Customer can also use *AWS CloudTrail* (AWS service that service that enables governance, compliance, operational auditing, and risk auditing of AWS account) for compliance auditing and security analytics for their AWS account activity, it can be easily integrated with customer applications using an API.
- Customer can also enable server access logs on *Amazon S3* (AWS storage service that provides object storage through a web service interface), which delivers access logs to them on hourly basis.
- *Amazon GuardDuty* (threat detection) analyzes logs from *AWS CloudTrail*, Virtual Private Cloud (VPC) Flow Logs and AWS Domain Name Service (DNS), to continuously monitor AWS accounts and workloads
- Further, Amazon Security Hub service can be used to centralize all the security functions and improve visibility into the organization.

- Azure:
  - Customer can use Azure Monitor logs which is a cloud-based IT management solution that helps manage and protect on-premises and cloud infrastructure. They can further integrate it with Log Analytics Security and Audit dashboard which provides a comprehensive view and categorizes its findings into security domains, notable issues, detections, threat intelligence and common security queries.

- Customer can record various types of logs through Azure like activity logs, Azure resource logs, Active directory usage logs, virtual machine logs, storage analytics, application insights and more.
- Azure features comprehensive logs to audit actions on resources. For example, through the Activity Log, customer can determine who initiated an operation, when it occurred, and what the status of the operation was.

Note to Customer: Both AWS and Azure offer tons of services for logging and monitoring at infrastructure level and again it is customer's responsibility to enable them and utilize them at system and application level. AWS logging and monitoring services are available via multiple tools as mentioned above and then all of them can be combined together through Amazon security hub for a complete view across the organization. Whereas for Azure, most of its logging and monitoring services are coupled with active directory, hence its more end user focused i.e. which actor is doing what, and Azure again provides a complete view through its log analytics and audit dashboard functionality. Approach for logging is different for both the players but gets the job done, AWS is more detailed from the application side whereas Azure is more detailed from the user side.

- **Equipment End of life**
  - AWS: At the end of life of a storage device, AWS decommissions it using techniques detailed in NIST 800-88. All media storage devices containing customer data are treated as high criticality assets and are treated accordingly throughout their life cycle and are not removed from AWS control until they have been securely decommissioned.

- Azure: At the end of a system's life, dedicated operational personnel follow rigorous and defined data handling and hardware disposal procedures to assure that hardware containing customer data is not made available to untrusted parties. This destruction process can be to disintegrate, shred, pulverize, or incinerate depending on the asset type.

Note to Customer: Both organizations invest heavily in safe disposal of the used media items, they have right policies and process in place for decommission and no media storage device is removed from their authority without being completely and securely decommissioned.

- **Data Encryption**
  - AWS:
    - Encrypt data at rest:
      - Customer can use the *AWS Encryption Software Development Kit (SDK)* with a customer master key (CMK) created and managed in *AWS Key Management Service (AWS KMS)* to encrypt arbitrary data. Encrypted data can be securely stored at rest and can be decrypted only by a party with authorized access to the CMK.
      - Another option is to encrypt Amazon Elastic Block Store (Amazon EBS) volumes and configure Amazon S3 buckets for server size encryption using AES-256 encryption. Both disk level and file system level encryptions are possible in AWS.

- Encrypting data using built in Linux libraries on Linux EC2 instance is also possible
- Data in an NVMe instance storage (Nonvolatile memory) is encrypted using an XTS-AES-256 block cipher implemented in a hardware module on the instance

- Encrypted data in Transit:
  - Customer can create a virtual private network (VPN) between their corporate data center to Amazon Virtual Private cloud (VPC) and protect the communication using several VPN connectivity options.
  - AWS provides HTTPS endpoints using the TLS (Transport Layer Security) protocol for communication, which provides encryption in transit when you use AWS APIs.
- Other Encryption tools available at AWS:
  - *AWS Key Management Service (AWS KMS)* which generates and manages both master keys and data keys, is used for server-side encryption of data and are FIPS 140-2 Level 2 validated
  - *AWS CloudHSM* (Cloud based hardware security module) allows customer to generate and use their own encryption keys on the AWS Cloud.
  - It also provides a client-side encryption library for implementing encryption and decryption operations on all types of data.

- *Amazon DynamoDB* (NoSQL database service) Encryption Client provides a client-side encryption library for encrypting data tables before sending them to a database service, such as Amazon DynamoDB.
- Linux DM-Crypt Infrastructure for kernel level encryption

- AWS follows Data Protection by design and by default.
  - Least privilege principle
  - Infrastructure as code: including security from the beginning of the design of architecture

- Azure:
  - *Azure Information Protection* helps customer to classify, label, and protect their documents and email. It can be done either automatically through administrators or manually by end users, customers can also do a combination of both by giving some predefined rules and recommendation options to end users. For example, if a user saves a file that contains sensitive information such as bank account number (after an administrator has predefined a rule to automatically recognize this kind of information), the user receives a notice that recommends applying a specific label to the file.
  - *Azure Key Vault*, a cloud-hosted service for managing cryptographic keys and other secrets used in cloud applications, provides capabilities to help customers with the protection of data and access to data. It enables customers to safeguard their cryptographic keys, certificates, and

passwords. It uses specialized hardware security modules (HSMs) for maximum protection and also supports a bring-your-own-key (BYOK) capability and its various related options. Customers can monitor and audit the usage of their stored keys using *Azure logging* which can also be incorporated to their existing security information and event management (SIEM) system for additional analysis, such as threat detection.

- Azure is developed using the Microsoft Security Development Lifecycle, which includes privacy-by-design and privacy-by-default methodologies
- Azure Storage Service Encryption allows customer to request that the storage service automatically encrypt the data when writing it to Azure Storage. All data is encrypted using 256-bit AES (Advanced Encryption Standard) encryption, also known as AES-256, one of the strongest block ciphers available
- For encrypting data inside virtual machines, customer can use Azure Disk Encryption for virtual machines that are hosted in Azure and have Windows or Linux running as a local operating system.
- Transparent Data Encryption with Azure SQL Database helps protect against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups, and transaction log files at rest.
- By implementing a Site-to-Site VPN with Azure, customers can create a virtual private connection between their on-premises network and an Azure Virtual Network. This connection takes place over the Internet and

allows them to securely "tunnel" information inside an encrypted link between customer network and Azure. Site-to-Site VPN is a secure, mature technology that has been deployed by enterprises of all sizes for decades and used IPsec tunnel mode.

- Microsoft offers another, even more secure connection option for cross-premises connectivity called Azure ExpressRoute, which is a dedicated WAN link between Azure and an on-premises location or an Exchange hosting provider

Note to Customer: Both AWS and Azure have data encryption protocols at all stages of data life cycle i.e. at rest and in transition. Azure offers default server-side encryption using 256 bits AES encryption, whereas AWS offers more isolated encryption options with customer master key to encrypt anything anywhere. Both offer encryption key management systems like AWS Key Management service or Azure Key Vault for better maintaining key secrecy and provide protected access to sensitive data. Azure supports customer in identifying and labeling sensitive data through it's in house Azure Information protection service, whereas AWS allows customers to create their own encryption master keys using AWS CloudHSM for encrypting arbitrary data. They both offer protected tunnels for encrypting data in transit and much more data encryption services for protection at every level.

- **Backup**
  - AWS:
    - AWS Backup is a fully managed backup service that makes it easy for customers to centralize and automate their backup of data across various

AWS services. It automates and consolidates backup tasks previously performed service-by-service along with configurable back up policies, thereby removing the need to create custom scripts and manual processes. With just a few clicks in the AWS Backup console, customers can create backup policies that automate backup schedules and retention management, enabling them to meet all business and regulatory backup compliance requirements.

- It is also PCI and ISO compliant as well as HIPAA eligible.

- Azure:
  - Azure Backup is a simple and secure built in cloud-integrated backup service offering to back up and restore customer's data. Customers can back up their SQL database and VMs running in Azure with just one click.
  - Azure has a Recovery Services vault which is a storage entity in Azure that houses data including data copies and configuration information for virtual machines, workloads, servers, and workstations.
  - Customers can manage their backup resources and activity from the Azure central backup management portal for easy administration. Azure backup can be easily compiled with Azure site recovery for restoring data centers in case of disaster recovery.

Note to Customer: Both AWS and Azure have easy to implement back up services which protects customer data and create immediate backups in minimum possible steps. Azure backup is simpler to use whereas AWS offers more flexibility with customizable automated back up policies.

Given the large number of benefits around scalability, efficiency, security, cost effectiveness and more, a lot many organizations are transitioning their computing infrastructure to cloud environment using IaaS delivery models with some of the leading CSPs. But choosing the right CSP for your cloud needs depends on many factors, security being one of the prime one. Customers also need to consider their business and technical requirements along with their current application technology stack, required industry certifications, support model, budget boundaries and more as these factors also play a very important role in finding the right cloud partner for your organization. So apart from security specific DP requirements, AWS and Azure are compared on these other factors as well:

- **Compliance**
    - AWS: Amazon works with lots of government agencies, and their compliance offerings include certifications in ITAR, DISA, HIPAA, CJIS, FIPS, and many more. They also provide security so that only screened persons can access the cloud, a must for agencies handling sensitive information.
    - Azure: Microsoft claims to have more than 50 compliant offerings, including ITAR, DISA, HIPAA, CJIS, FIPS. Microsoft provides the same level of security as Amazon, setting up permissions so that only screened persons can access a government-level cloud.

Note to Customer: Both organizations have almost every possible compliance certification be it federal or vertical specific, as they both serve sensitive clients all across the world.

- **Accessibility:**
    - AWS:
        - AWS offers wide breadth and depth of services, with more than 175 across compute, storage, database, analytics, networking, mobile, developer tools, management tools, IoT, security and enterprise applications, AWS offers a lot of power, flexibility and customization room with support for many third-party integrations.
        - However, AWS comes with some learning curve to understand and take advantage of these powerful customizations. (Mogull, 2019)
    - Azure:
        - Azure offers more defined model with less flexibility for customization but is easier and familiar to use directly out of the box, especially for Windows platform organization as it doesn't require learning something new. It is simple to integrate on-premises Windows servers with cloud instances to create a hybrid environment. And common windows tools such as SQL database and Active Directory work well with Azure. (Mogull, 2019)

Note to Customer: Both organizations offer some great tools and services in their IaaS delivery mode, it depends on the customers business and technical requirements. AWS offers more powerful and customizable services but requires some learning curve whereas Azure is more of a standard offering and integrates easily with existing windows environment.

- Pricing & Support Model:
    - AWS:
        - Servers are charged per second of usage (Churchman, 2020)
        - As per its customizable offerings, it becomes difficult for organizations to comprehend the metrics and pricing & support model as per customized architectural configurations. AWS understands this pain point of certain customers and offers an AWS pricing calculator for better estimations.
        - In terms of support, AWS is known for excellent support services with clearly defined documentation for self-service.
    - Azure:
        - Servers are charged per minute of usage
        - Standard pricing structures and flat billing rate
        - Offers great deals and discounts to existing windows customer base (Churchman, 2020)
        - Azure tends to lack in terms of consistency for its support services and online documentation.

Note to Customer: AWS definitely has first movers' advantage in the market with more features, customizations and excellent documentation and support models. Azure is moving pretty quickly with more standard and easier to integrate with offerings.

- Open source connectivity:
    - AWS: AWS is excellent for open source developers as it welcomes Linux users and offers several integrations for different open source applications.
    - Azure: Azure has now become more accessible to open source community and works equally well with windows, Linux and MacOS.

Note to Customer: AWS's technological superiority showcases its close connectivity to open source community, but Azure is certainly catching up real fast. More open-source-centric or DevOps-centric customer tends to prefer AWS over Azure.

There can certainly be more factors of comparison between AWS and Azure, but we will stop here as per the scope of this research paper.

Conclusion

Data Privacy is a factor of prime importance, especially when dealing with European data subjects and organizations. Most of the big CSPs are getting all of their cloud services complaint in GDPR regulation so as to work in EU region. We did a deep dive into analyzing GDPR DP requirements in cloud environment, segregated it further into customer and CSP responsibilities as per CISPE code of conduct. And then did a detailed analysis of security specific DP responsibilities on world's biggest IaaS providers by market share (Mogull, 2019) – Amazon Web Services and Microsoft Azure.

Table III

AWS v. Azure

	Amazon Web Services (AWS)	**Microsoft Azure**
Strengths	• Greatest global reach with longest record of reliable cloud service. • AWS offers a lot of power, flexibility and customization room across 175 services with support for many third-party integrations. • More open source centric, get access to latest technology • In terms of security, highest level of isolations possible. Default access	• Azure is more accessible to work with, especially for windows enterprise. Comparatively, easier learning curve. • Works better in hybrid environment (more than 1 CSP) • Azure active directory acts as a single source of truth, all tools/services are integrated with this, hence easy management and can be easily combined with an

	for any service is restricted, unless specified by the administrator. • Clear and concise documentation available online for self-help along with highly rated support services. • Customer can write customizable policies and can create their own encryption key.	organizations' existing infrastructure • Flat pricing structure and offers great discounts to existing windows customers • Easier Identity and access management through active directory.
Weaknesses	• It requires a learning curve to take advantage of its flexible and customization features. • More isolated services make enterprise level scale management difficult. Though AWS launched AWS security hub to provide a combined view of all tools and services. • No standard pricing structure, it depends on the selection and customizations of tools/services.	• Poor documentation and lack of consistency in support services. • Lower security: Less isolation among services and it starts with default "allow" for most of its services, as its all connected to active directory. • Less flexibility and fewer customization options.

Both AWS and Azure offer competing features and benefits with excellent customer reviews and showcase complete adherence to GDPR requirements. They both have all required privacy compliance certifications and work with sensitive clients all around the world, including a number of GDPR related successful projects. Both of them can support customers in reaping multiple benefits of hyper scalable cloud solution, it all depends on customer's business requirements.

Since both configuration and integration are effortless in Azure, I believe it would be a good match for first time clouds users and startups, and also windows operated enterprises as Azure comes with default integration with Microsoft products like Active directory and SQL database. AWS is ideal for mature players and large companies which need flexibility with wide range of services as per their different requirements, are more technologically sophisticated and require more security controls across various functions/geographies.

Future Research

For the purpose of future research, I would like to propose following ideas in addition to this research:

- Comparison between GDPR DP requirements and California Consumer Privacy Law (CCPA) requirements and if above mentioned AWS and Azure services (as per CISPE) are enough to maintain compliance with both the regulations? This would also include contrast between EU and US privacy landscape.
- Add Google Cloud Platform to the comparison table with AWS and Azure, as it is coming up with the most economical pricing model of all three along with advanced machine learning capabilities and hybrid cloud environment.

- Study some past GDPR related security breaches and analyze vulnerable security services/controls provided by major CSPs. This would also include share of responsibilities taken by customer and CSP as per court's final decision.
- Apart from EU and US, study privacy regulations of all other major countries as well and develop a common privacy regulation framework which can provide worldwide privacy and data protection assurance.
- Suggest changes to GDPR application as per evolving technology landscape, like how GDPR will change in the realm of quantum computing when data encryption will not be of much value.

References

Ramgovind, S., Eloff, MM., & Smith, E. (2010). The Management of Security in Cloud Computing. *IEEE*.

Deyan, C., & Hong, Z., (2012). Data Security and Privacy Protection Issues in Cloud Computing. *ICCEE*.

Duncan, B. (2018). Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing?. IARIA. *Cloud Computing 2018*.

Shucheng, Y., Cong, W., Kui, R., & Wenjing, L., (2010). Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. *IEEE INFOCOM*.

B. Russo, L. Valle, G. Bonzagni, D. Locatello, M. Pancaldi and D. Tosi. (2018) Cloud computing and the new EU general data protection regulation, *IEEE Cloud Comput.*, vol. 5, no. 6, pp. 58-68.

General Data Protection Regulation (GDPR) – Official Legal Text. (2019, September 2). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

CISPE.cloud. (2017, January). *Data Protection: Code of Conduct for Cloud Infrastructure Service Providers*. https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

Microsoft. (2019, October). *Shared Responsibility for Cloud Computing*. https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Amazon Web Services. (2017, May). *Amazon Web Services: Risk and Compliance*. https://aws.amazon.com/security/

Amazon Web Services. (2019, October). *Navigating GDPR Compliance on AWS*. https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf

Microsoft. (2017, May). *How Microsoft Azure Can Help Organizations Become Compliant with the EU General Data Protection Regulation (GDPR)*. https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr?view=o365-worldwide

Mogull, R. (2019, November 6). *AWS vs. Azure vs. GCP: A Security Pro's Quick Cloud Comparison*. DisruptOps. https://disruptops.com/aws-vs-azure-vs-gcp-a-security-pros-quick-cloud-comparison/

Ceroici, M., Nebuloni, G., Brown, D. (2017, July). *Implications of the EU Cloud Code of Conduct on European Cloud Infrastructure*. IDC Central. https://www.ibm.com/downloads/cas/OQWOZBMV

Nebuloni, G. (2017, May). *Implications of the Code of Conduct for Cloud Infrastructure Service Providers in Europe*. IDC Central. https://d1.awsstatic.com/whitepapers/compliance/Implications_of_the_Code_of_Conduct_for_CISPE.pdf

Churchman, M. (2020, January 28). *Cloud Security Considerations for AWS, Azure, & Google*. Sonrai Security. https://sonraisecurity.com/education/aws-azure-google-cloud-security-iam/