Footprints: Privacy for Enterprises, Processors, and Custodians…Oh My!

Blair Witzel & Carrie Mount***

ABSTRACT

Americans' interest in privacy—as evidenced by increasing news coverage, online searches, and new legislation—has grown over the past decade. After the European Union enacted the General Data Protection Regulation (GDPR), technologists and legal professionals have focused on primary collectors of data—known under various legal regimes as the "controller" or "custodian." Thanks to advances in computing, many of these data collectors offload the processing of data to third parties providing data-related cloud services like Amazon, Microsoft, and Google. In addition to the data they have already collected about the data subjects themselves, these companies now "hold" that data on behalf of other companies and are known under the GDPR infrastructure as "processors."

In this context of technology giants processing data for other companies, the current focus on privacy rules for primary data collectors seems almost misplaced. What are these companies required to do? Instead of focusing on the data collectors, the community should ask how transparent the data holders are in their demonstration of compliance. This Article seeks to explore that question through a comparative analysis of the publicly available privacy compliance documentation. Further, it will analyze the companies that Gartner's May 2018 "Cloud Quadrant"

* Senior Lead, MD&A Health. The author would like to thank Kerry Lyon for her unwavering support in the development of this Article and related projects, and Dr. Tracy Kosa, Adjunct Professor at Seattle University School of Law, for her helpful suggestions and editorial contributions.

** J.D. Candidate, 2019, Seattle University School of Law; Managing Editor, *Seattle University Law Review*. I am grateful to Dr. Tracy Kosa, who inspired my interest in the GDPR and provided insightful suggestions for this Article. I would also like to thank my brilliant co-author, Blair Witzel. Finally, I would like to thank Leila Javanshir for her organization of *Seattle University Law Review*'s annual Spring Symposium, which brought together many outstanding members of the privacy law community, and the *Seattle University Law Review* staff for its commitment to publishing topical scholarship.

identifies as the leaders in the data processing environment: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.

CONTENTS

I. THE SETTING

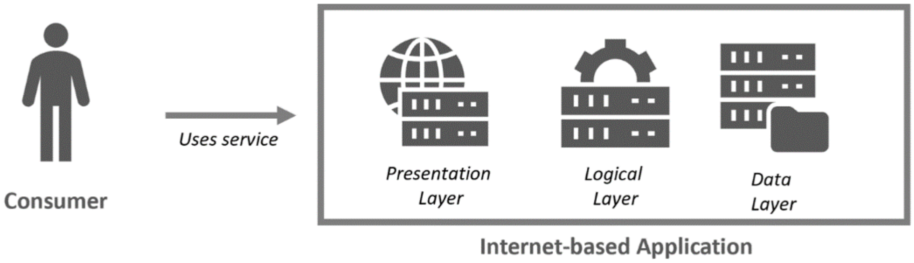
This Article will proceed in five parts. Part I will address scope, standard data flows, and applicable terminology, including legally significant terms. Part II will outline mechanisms for complying as a cloud provider, including requirements under the European Union's General Data Protection Regulation (GDPR) and concordant obligations for providers. Part III sets out evaluation criteria for the top three leaders in cloud services and considers each in turn. Part IV provides a framework for assessing risk and tests it in separate scenarios using the GDPR obligations outlined earlier. This Article concludes with some insights for controllers to consider when utilizing cloud services.[1]

To begin, the ever-evolving landscape of both cloud technology and privacy necessitates a section dedicated to the nomenclature of these topics.

A. The Cloud

The terms "cloud" and "cloud computing" have become catch-all phrases that cover a multitude of cloud-based services. For the purposes of this Article, we will use the term to include a myriad of services provided by the top three cloud service providers, including computation, database, storage, content delivery, analytics (or "big data"), mobile, networking, and security or identity services, as well as monitoring and management of said services.

Standard Data Flow



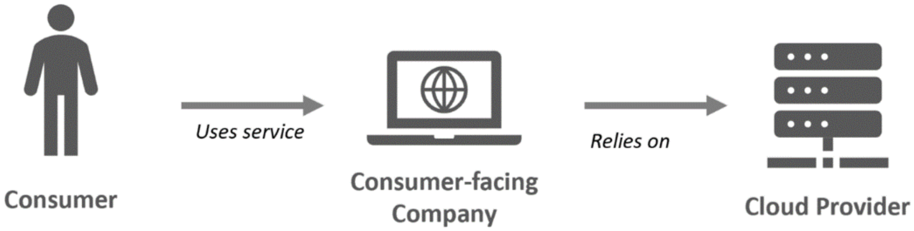
The technical architecture for internet-based applications exists in three key domains, also known as tiers or layers.[2] They are the presentation layer, the logical layer, and the data layer.[3] The presentation layer is what the consumer sees. The logical layer is the "thinking" layer, which processes the information and makes decisions and calculations. The data layer is where the information is stored. These layers work together to provide an internet-based application to a consumer. When a consumer inputs personal information (PI) into an internet-based application, the PI is entered in the presentation layer, processed by the logical layer, and stored in the data layer.

[1] Notably, a detailed analysis of the market's response to privacy-related news with respect to cloud service providers is outside the scope of this Article (but merits consideration in context), as is a detailed consideration of enforcement patterns or decision-making by the regulatory body in the United States (the Federal Trade Commission) or other countries.

[2] Heiko Schuldt, *Multi-Tier Architecture*, *in* ENCYCLOPEDIA OF DATABASE SYSTEMS 82 (Ling Lui & M. Tamer Özsu eds., 2009).

[3] *See generally* CHRISTOPH FEHLING ET AL., CLOUD COMPUTING PATTERNS: FUNDAMENTALS TO DESIGN, BUILD, AND MANAGE CLOUD APPLICATIONS (2014).

Cloud providers offer various models for the technical services that they provide.[4] Cloud providers can and do provide a variety of technical services that are required to make up an internet-based application.[5] Some focus strictly on providing the data layer, whereas others provide a broader set of technical services at the logical layer. Therefore, the technical relationship between the consumer-facing company and the cloud provider will vary depending on the needs of the company's consumers and the capabilities of the cloud provider. Simply put, a consumer uses a consumer-facing company's application, which in turn uses a variety of technical services (usually from the logical and data layers) from a cloud-based provider to support delivery of the consumer-facing application.



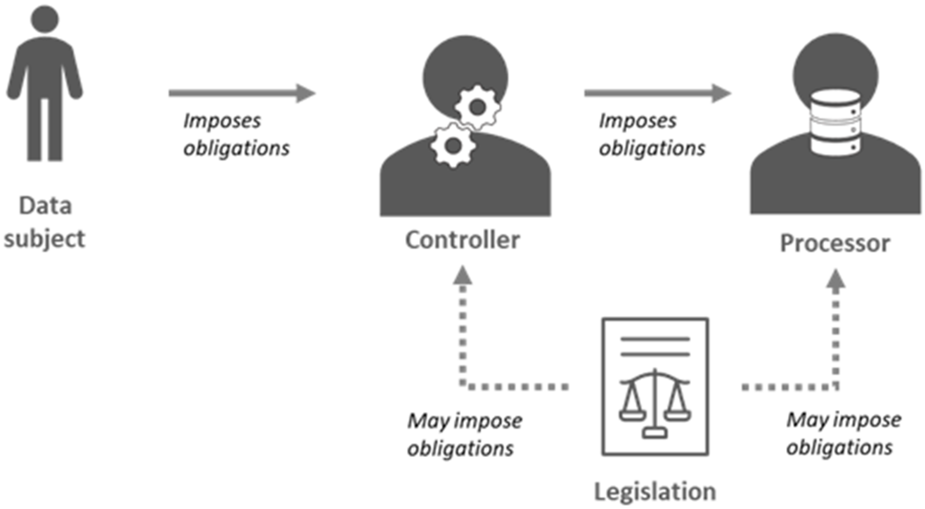
Summarizing the technical relationship as such helps us to describe a simplified business relationship among the parties and better discuss the relevant privacy obligations. A consumer provides personal information to the consumer-facing company in the course of receiving the services and is known as the data subject. The consumer-facing company providing the application has the business relationship with the consumer and controls how the PI will be used. The consumer-facing company is therefore considered the controller.[6] The controller in turn has a business relationship with the cloud provider, who is *not* authorized to use the PI for its own purpose. That cloud provider is further restricted from using the PI for any purpose not authorized by the controller or required by legislation. It is therefore considered the processor.[7]

[4] *See* ERIC SIMMON, NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUBLICATION 500-322: EVALUATION OF CLOUD COMPUTING SERVICES BASED ON NIST SP 800-145 (2018).

[5] Phil Goodwin, *Five Capabilities to Look for in a Cloud Storage Provider*, TECHTARGET (Feb. 2014), https://searchstorage.techtarget.com/tip/Five-capabilities-to-look-for-in-a-cloud-storage-provider [https://perma.cc/ZTH4-VJAR].

[6] Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

[7] *Id.* art. 4, at 33.



Thus, the privacy relationship flows from the business relationship. The legal requirements impose obligations on the controller that it must meet to protect the privacy of the data subject. The controller flows any relevant obligations on to the processor to ensure that the controller is able to meet its obligations in protecting the data subject's privacy. Grasping the contours of the data-protective GDPR is key for all professionals interacting with companies subject to its requirements.

B. Regulatory Context

In 2018, cloud providers became subject to far more regulation in their data processing activities than ever before. The legal setting in which cloud providers operate informs the decisions of players from high-level managers to customers seeking to house or process their data on a cloud-based platform. Understanding the framework and requirements of the Regulation[8] is critical in evaluating the relationships, obligations, and potential risks facing cloud providers and their customers.

GDPR: Scope and Roles

The GDPR went into effect in May 2018, carrying with it far-reaching consequences for businesses who gather data from European Union (EU) residents. The scope of the GDPR protects EU data subjects[9] outside the borders of the EU:

[8] *Id.*

[9] A data subject is a natural person. *See id.* Recitals 1–19, at 1–4.

> [The GDPR] applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behaviour takes place within the Union.[10]

In the context of cloud computing companies, many of which are considered "processors," the GDPR imposes new obligations and allows for penalties resulting from non-compliance. In order to understand the scope of the GDPR, the explanation of these important roles is helpful.

Simply stated, under the GDPR, a "controller" is a person or entity that "determines the purposes and means of the processing of personal data."[11] Any company that collects personal data for use in its business processes is likely a controller. For example, if an Etsy seller collects its customers' addresses, payment information, and names, that seller is a controller. The GDPR imposes myriad obligations on controllers, many of which require careful diligence in the selection and monitoring of their processors.[12]

A key change in EU privacy law with the enactment of the GDPR is that processors face previously absent obligations and are subject to a number of penalties for non-compliance.[13] A "processor" is defined in the GDPR as an entity that processes this data on behalf of the controller.[14] The Regulation provides a non-exhaustive list of what constitutes processing, whether automated or by a person, including "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[15] Processors act at the direction of their customers, who are generally the controllers of the data. The wide range of activities considered "processing" under the Regulation demonstrates the GDPR's application to cloud-based providers and their designation as processors.

Additionally, a company may be both a controller and a processor. For example, a company that provides more than one cloud service to its customers may be both controlling and processing data. An example is Amazon Web Services (AWS), which acts as a processor when providing infrastructure, storage, and analytics at the direction of its customers, and

[10] *Id.* art. 3(2), at 33.

[11] *Id.* art. 4(7), at 33.

[12] *See id.* art. 28, at 49.

[13] *See id.* art. 77, at 80; *id.* art. 79, at 80; *id.* art. 83, at 82–83; *id.* art. 84, at 83.

[14] *Id.* art. 4(8), at 33.

[15] *Id.* art. 4(2), at 33.

also acts as a controller when it collects, stores, and uses its customers' data. The GDPR has blurred the line in the controller–processor relationship because many of the obligations once imposed only on controllers now fall on the shoulders of processors; these obligations are discussed in detail and illustrated through case studies below.

II. COMPLYING AS A CLOUD PROVIDER

Cloud providers, who almost always act as processors, are mandated to execute a variety of actions to effectuate the principles of the GDPR. Given the increased responsibility of processors to both controllers and data subjects, an explanation of the Regulation's requirements is critical to ensure cloud providers, and those who advise them, are compliant with the now omnipresent GDPR.

Legal Requirements Under the GDPR

The GDPR's enactment carries obligations for processors that previously only affected controllers—and most processors who sit outside the EU are subject to the GDPR.[16] Foremost, the Regulation requires controllers to only use a processor that can provide "sufficient guarantees" that it has implemented "appropriate technical and organisational measures" to protect the data subject's rights and comply with the GDPR.[17] What standards or assurances would qualify as sufficient guarantees are not outlined by the GDPR, and each controller must use its best judgment to determine whether the processor has provided adequate assurances. Because of this, the risk exists that controllers will fail to investigate the processors' promises of compliance or lack the sophistication to understand the processors' purported safeguards. Similarly, what will be considered appropriate technical and organizational measures to comply with the Regulation are undefined in the GDPR. While this vague language allows cloud providers with varying purposes and customers to consider what is appropriate in each set of circumstances, the lack of clarity may promote a decline in rigor in the absence of specific standards.

The GDPR mandates a legally binding contract between the processor and the controller, often called the "Data Processor Agreement" (DPA), that outlines "the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and

[16] The GDPR contains a provision repealing Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281), which enforced nearly all consequences on data controllers, but not data processors.

[17] GDPR, *supra* note 6, art. 28, at 49.

categories of data subjects and the obligations and rights of the controller."[18] Additionally, the DPA must contain the processor's agreement to several obligations, which are discussed in further detail below. The processor must stipulate in the DPA that it will only process data at the direction of the controller, that the processor's employees are compliant with the Regulation's principles (including confidentiality), that the processor will not engage sub-processors without prior controller authorization, that the processor will follow controller instructions to delete or return data at the end of the agreement, and that the processor will make information available to the controller to demonstrate compliance with the Regulation.[19] The processor is also required to assist the controller in meeting its obligations under the GDPR through "appropriate technical and organizational measures." The processor must assist the controller in not violating the rights of the data subject as well as in complying with the obligations pursuant to Articles 32 through 36.[20] This mandatory agreement provides specificity to otherwise expansive GDPR obligations and assigns responsibility to the respective controller and processor.

When processors engage sub-processors, the controller must have provided prior written consent to the sub-processing arrangement.[21] While a processor may include language in their DPA generally authorizing the use of sub-processors, the controller must still be notified of new sub-processors and have time to express objections regarding the sub-processor.[22] Further, sub-processor agreements must impose the same responsibilities to which the processor is subject; however, the processor maintains vicarious liability for actions taken by the sub-processor.[23]

Transparency and the demonstration of compliance are important principles in the GDPR. Accordingly, processors must maintain records containing the name and contact information of the processor and the controllers for whom it processes, the categories of processing it engages in for each controller, information relating to any transfers of data to third countries (countries outside the EU), and "a general description of [its] technical and organisational security measures."[24] If a processor has less

[18] *Id.* art. 28(3), at 49.

[19] *Id.* arts. 28(3)(a)–(b), (d), (g)–(h), at 49.

[20] *Id.* arts. 28(e)–(f), at 49. Articles 32 through 36 address, respectively, security of processing, notification of data breaches to both authorities and the data subject, data protection impact assessments, and prior consultation with supervisory authorities if warranted after the impact assessment. *See id.* arts. 32–36, at 51–54.

[21] *Id.* art. 28(2), at 49.

[22] *Id.*

[23] *Id.* art. 28(4), at 50.

[24] *Id.* arts. 30(2)(a)–(d), at 50–51.

than 250 employees, it is not subject to the foregoing obligations with respect to demonstrating compliance unless its processing activities are "more than occasional," pose a likely risk to the data subject, or process sensitive information.[25]

The Regulation imposes increased data breach notification requirements on processors. Under Article 34, processors are required to notify controllers "without undue delay" once the processor becomes aware of a breach.[26] Although the undefined timeframe may frustrate some processors, it may allow for more complete notifications and responses if processors are not rushing to meet a set time-to-notification requirement. Controllers face other breach notification obligations, including a defined timeframe to notification and the contents and delivery methods the notifications to data subjects must take. A controller's obligations are outlined in Articles 33 and 34.[27]

Processors are required to use and maintain "appropriate" technical and organizational security measures in order to protect the rights of data subjects.[28] Article 25, titled "Data protection by design and by default," imposes the obligation on controllers to "integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."[29] Given that controllers may only use processors who demonstrate their adherence to the Regulation, these responsibilities for appropriate security and technical measures are passed to processors. The relevant provisions do not spell out specific standards but emphasize data minimization as a guiding principle and that pseudonymization can assist that goal.[30] Additionally, approved certifications, allowed under Article 42,[31] may demonstrate compliance with Article 25's requirement of data protection by default and design.[32]

Transfers of data to non-EU countries, or "third countries," is permitted under Articles 45 and 46 if the third country has been deemed adequately protective through an "adequacy ruling"[33] or if appropriate safeguards are present to ensure compliance with the Regulation.[34] Article

[25] *Id.* art. 30(5), at 51.

[26] *Id.* art. 33(2), at 52.

[27] *Id.* arts. 33–34, at 52–53.

[28] *Id.* art. 25(1), at 48.

[29] *Id.*

[30] *Id.*

[31] *Id.* art. 42, at 58.

[32] *Id.* art. 25(3), at 48.

[33] *Id.* art. 45(1), at 61 (providing that a transfer may take place where the "Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization").

[34] *Id.* arts. 45–46, at 61–62.

45 provides a non-exhaustive list of criteria the Commission uses to assess adequacy, including the legal and social framework of the country,[35] enforceability of data privacy rights, and international commitments to which the third country is a signor, such as treaties related to data protection.[36] In absence of an adequacy ruling, a processor may show appropriate safeguards through binding corporate rules, EU-generated model contractual clauses, and approved certifications.[37] The United States is not considered an adequately secure country for data transfers, but many U.S. companies choose to certify under the Privacy Shield, an EU–U.S. compact that certifies a U.S. entity is adequately compliant with a high standard of data protection.[38]

A processor may be required to appoint a data protection officer (DPO) if the processor is a public authority or body, if its processing encompasses large-scale regular monitoring of data subjects, or if it processes especially sensitive personal data (as defined under Article 9).[39] DPOs must be employed "on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices" in order to execute their responsibilities as outlined in Article 39.[40] A DPO is mandated to provide advice for and monitoring of the processor's compliance with the Regulation; the GDPR also requires the DPO assist and cooperate with a supervisory authority as required.[41]

[35] The Commission considers the legal and social factors such as

> the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred.

Id. art. 45(2)(a), at 61.

[36] *Id.*

[37] *See* Michelle Rosenberg, *Cross-Border Transfers of Personal Data in Light of GDPR*, FOX ROTHSCHILD LLP (Mar. 23, 2018), https://dataprivacy.foxrothschild.com/2018/03/articles/european-union/gdpr/cross-border-transfers-of-personal-data-in-light-of-gdpr/ [https://perma.cc/QZ9N-SHGP].

[38] *Id.*

[39] GDPR, *supra* note 6, art. 37(1), at 55. Article 9 defines the most sensitive data as information relating to the data subject's "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." *Id.* art. 9(1), at 38.

[40] *Id.* art. 37(5), at 55.

[41] *Id.* art. 39(1), at 56.

III. KEY PLAYERS

Cloud service companies provide what are often called "Infrastructure as a Service" (IaaS) products. According to information technology (IT) consulting firm Gartner, the IaaS market grew 29.5% between 2016 and 2017—from $18.2 billion to $23.5 billion.[42] While there is some criticism of these reports, including a lack of transparency around funding, methodological questions,[43] and a lack of consideration of open source vendors,[44] Gartner nonetheless provides a reasonably influential and oft-cited rating of technology vendors.[45] Of particular relevance in identifying cloud service providers is the "Leadership" rating. In 2018, the Gartner report updated its ratings and identified Amazon, Microsoft, and Google as Leaders in Cloud Infrastructure as a Service (Worldwide).[46] We selected the same for our analysis.

A. EVALUATION CRITERIA

For comparison purposes, we set out three criteria to review each of the cloud service providers as follows:

[42] *Gartner Says Worldwide IaaS Public Cloud Services Market Grew 29.5 Percent in 2017*, GARTNER (Aug. 1, 2018), https://www.gartner.com/en/newsroom/press-releases/2018-08-01-gartner-says-worldwide-iaas-public-cloud-services-market-grew-30-percent-in-2017 [https://perma.cc/5ZH8-U4WD]. Gartner publishes a market research report series, the *Magic Quadrant*, on specific technology industries that analyze market trends. *Gartner Magic Quadrant*, GARTNER, https://www.gartner.com/en/research/methodologies/magic-quadrants-research [https://perma.cc/8NL5-FANH].

[43] *See*, *e.g.*, Tony Byrne, *Looking Beyond the Magic Quadrant to Find the Nitty-Gritty*, REAL STORY GROUP (Aug. 7, 2009), https://www.realstorygroup.com/Blog/1660-Looking-beyond-the-magic-quadrant-to-find-the-nittygritty [https://perma.cc/KZP8-BM4L].

[44] *See, e.g.*, *Vendor Complains in a Very Public Blog Post About Gartner's Data Integration Magic Quadrant*, SAGECIRCLE (Dec. 29, 2008), https://sagecircle.com/2008/12/29/vendor-complains-in-a-very-public-blog-post-about-gartners-data-integration-magic-quadrant/ [https://perma.cc/H7NH-NYNK].

[45] The Gartner report generates additional industry coverage. *See, e.g.*, Janakiram MSV, *10 Key Takeaways from Gartner's 2018 Magic Quadrant for Cloud IaaS*, FORBES (Jun. 2, 2018), https://www.forbes.com/sites/janakirammsv/2018/06/02/10-key-takeaways-from-gartners-2018-magic-quadrant-for-cloud-iaas/#5825e60c14df [https://perma.cc/2LNB-WUR4]; Laura Shiff, *Gartner Magic Quadrant for Cloud Infrastructure as a Service 2018*, BMC BLOGS (Sept. 5, 2018), https://www.bmc.com/blogs/gartner-magic-quadrant-cloud-iaas [https://perma.cc/4CE4-YSX2]. The Gartner report is also cited by service providers as part of sales and marketing materials. *See, e.g.*, *See Why Gartner Named Google a Leader a Second Year*, GOOGLE CLOUD, https://gsuite.google.com/campaigns/gartner-magic-quadrant-ccp-2018/ [https://perma.cc/RS29-5ACR].

[46] Dennis Smith, Lydia Leong & Raj Bala, *Magic Quadrant for Cloud Infastratue as a Service, Worldwide*, GARTNER (May 23, 2018), https://www.gartner.com/doc/reprints?id=1-50WJ5DV&ct=180525&st=sb [https://perma.cc/JU4Y-SXCH].

#	*Criteria*	*Explanatory Note*
1	Transparency	What documentation is available on the website (without login, registration, or signing a nondisclosure agreement)? Does the content go beyond simple affirmative statements, e.g., "privacy is important," to include actual commitments, evidence of commitments, or both? We look for audit reports or assessments and statements of compliance.
2	Readability	Are the documents readable to a layperson, or is a certain level of expertise (legal or technical) necessary? We used http://readabilityscore.com to help inform and guide our analysis for consistency.[47] We look for discoverability, document length, and simple navigation.
3	Accountability	Does the provider meet its GDPR requirements? If so, how does the provider meet its GDPR requirements? Do the documents specifically outline the relationship and obligations between the data controller and processor? Similarly, do they explicitly list options for the data controller in selecting certain privacy protections?

Overall, we seek to provide an evaluation of whether the documents are understandable and what they actually say, as opposed to what the perceptions of obligations may be.

B. Amazon Web Services

Amazon Web Services, known as "AWS," provides "a secure cloud services platform, offering compute power, database storage, content delivery and other functionality" to its customers, who are in most cases data controllers.[48] Gartner declared AWS "the clear leader in the worldwide IaaS market with an estimated $12.2 billion revenue in 2017, up 25% from 2016."[49] A Synergy Research Group study estimated that

[47] The site provides readability scores, readability grade level scores, and overall text statistics. We focus our analysis on the Flesch-Kincaid readability and grade level. For more information on the Flesch-Kincaid method, see *Flesch-Kincaid Readability Tests*, WIKIPEDIA, https://en.wikipedia.org/w/index.php?title=Flesch–Kincaid_readability_tests&oldid=873334575 [https://perma.cc/9LB5-UB3M].

[48] *What is AWS?*, AMAZON WEB SERVICES, https://aws.amazon.com/what-is-aws/ [https://perma.cc/32AC-G48L].

[49] *Gartner Says Worldwide IaaS Public Cloud Services Market Grew 29.5 Percent in 2017*, *supra* note 42.

AWS has held over 30% of the market share for over three years.[50] Given its broad customer base and vulnerability to scrutiny, it is no surprise that AWS has published extensively on GDPR compliance.[51] As a processor, AWS has developed the "GDPR Center"—which features blog posts, a podcast, videos, and white papers—to announce its compliance with the GDPR and to address controllers' responsibilities.[52]

The GDPR Center addresses AWS's compliance as a processor and highlights AWS products and features that allow controllers to comport with the GDPR. Specifically, the website lists the following "features and services" that AWS customers can use "as they seek to comply with the GDPR": encryption, monitoring and logging, access controls, data privacy, security, and compliance programs.[53] Two documents in particular are useful to analyze for accessibility to controllers: AWS's GDPR white paper, *Navigating GDPR Compliance on AWS*,[54] and a blog post, *All AWS Services GDPR Ready*,[55] which was published two months ahead of the GDPR entering into force.

1. Transparency

The GDPR Center contains many documents, charts, and resources to enable customers (who are, for GDPR purposes, the data controllers) to make decisions about whether AWS is able to demonstrate, as required by Article 28, that it has appropriate technical and organizational safeguards in place to comply with the GDPR.[56] All of the information is available without a log-in or account, making the AWS compliance information extremely transparent. If processors restrict controllers' ability to access GDPR information, then controllers are less able to make informed decisions when selecting processors.[57] The documents, which are discussed below, are readily available in the GDPR Center with a clean interface and clear titles. The search function was not very helpful; we had

[50] *Cloud Growth Rate Increased Again in Q1; Amazon Maintains Market Share Dominance*, SYNERGY RESEARCH GRP. (Apr. 27, 2018), https://www.srgresearch.com/articles/cloud-growth-rate-increased-again-q1-amazon-maintains-market-share-dominance [https://perma.cc/SKR3-3MBE].

[51] *See id.*

[52] *General Data Protection Regulation (GDPR) Center*, AMAZON WEB SERVS., https://aws.amazon.com/compliance/gdpr-center/ [https://perma.cc/H82Q-9WPL].

[53] *Id.*

[54] AMAZON WEB SERVS., NAVIGATING GDPR COMPLIANCE ON AWS (2018) [hereinafter WHITE PAPER], https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf [https://perma.cc/VAJ8-YDY2].

[55] Chad Woolf, *All ASW Services GDPR Ready*, AMAZON WEB SERVS.: SECURITY BLOG (Mar. 26, 2018), https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/ [https://perma.cc/966N-4W3D].

[56] GDPR, *supra* note 6, art. 28, at 49.

[57] An extreme example is the requirement of a nondisclosure agreement prior to accessing the GDPR compliance information.

to filter the results to blog posts only to find information related to our test phrase, "data processing addendum," but we did find most of what we sought quickly through links on the front page of the GDPR Center.

2. Readability

Although no particular *legal* knowledge is needed to understand the white paper or the blog post, as they allude to the need to comply with the GDPR and briefly describe the Regulation; nevertheless, the reader likely needs a relatively high level of *technical* knowledge in order to understand the documents. AWS's white paper was scored under the Flesch Reading Ease system at 33.3 and earned a Flesch-Kincaid Reading Grade Level score of 15—these scores indicate at least a college graduate level education is required and are classified as "very difficult to read." The readiness blog post, on the other hand, scored a 22.1 and a 17.6 on the tests, respectively, indicating a more easily understood document.

While the white paper would be extremely difficult for a lay person to understand, the purpose of a white paper in a processor selection situation is most likely to allow an information technology professional to assess AWS's safeguards and products. As such, the reading level, while high, may be appropriate given the need to make informed decisions as a controller. Further, the specific technical information supports the white paper's transparency, as it does not make sweeping or broad statements about compliance but provides information on certifications, technical specifications, and products that controllers may add based on their needs to heighten data protection in compliance with the GDPR.

On the other hand, the blog post, which links to and summarizes much of the white paper, is written with a conversational style, utilizes bullet points, and is one-eighth the length of the white paper.[58] Featured prominently on the GDPR Center's main page, the blog post is likely a first read for many controllers who are researching processors' GDPR compliance. The much more readable tone and level make it a stepping stone on the path to the more technical white paper while still providing important GDPR information. The blog post links to a GDPR-compliant Data Processing Addendum, certifications, conformity to a code of conduct, and AWS products allowing controllers to guard higher risk data or uses.[59]

[58] Woolf, *supra* note 55.

[59] *Id.*

3. Accountability

The processor–controller relationship is explicitly defined in the white paper and further discussed in the linked Data Processor Addendum (DPA), which AWS describes as GDPR-compliant.[60] AWS incorporated the DPA into its AWS service terms to ensure all users subject to the GDPR have entered into the mandated processor–controller agreement. The white paper reminds controllers that, when using cloud services, "security responsibilities become shared between you and your cloud service provider . . . . AWS is responsible for securing the underlying infrastructure . . . and you are responsible for anything you put on the cloud or connect to the cloud."[61] AWS outlines its security responsibilities and claims, "[p]rotecting this infrastructure is AWS's number one priority."[62] Although visiting the physical data centers is not permitted, third-party auditor reports are available to controllers; the auditor reports do not appear to be available without contacting AWS.[63]

The white paper is extremely detailed in what protections AWS has implemented as a processor, as well as products and features it offers to controllers, thereby requiring the aforementioned technical knowledge to understand much of the document. It makes references to the various GDPR provisions with which AWS must comply as a processor but does not map to the Regulation exactly. The white paper discusses Article 25, which requires safeguards processors must put in place, and describes the features AWS provides to controllers, including granular access, which allows varying permissions for different users,[64] temporary access capability, multi-factor authentication, API request authorizations, geo-restrictions, and temporary access tokens.[65] Additionally, the document details AWS's ability to pseudonymise and encrypt data.[66]

In regards to reporting and logging, as required by the GDPR, AWS explains its services that allow controllers to detect and track breaches, the option to use its Cloud Trail product to trace an API calls' origination, location, and time, and its AWS Config product that provides a detailed report of resource configuration.[67] AWS states in the white paper that it is aligned with security best practices and many IT standards, including SOC 1, SOC 2, and SOC 3. Additionally, it describes AWS's options allowing for compliance with sector-specific standards, such as HIPAA and

[60] WHITE PAPER, *supra* note 54, at 2.

[61] *Id.* at 11.

[62] *Id.*

[63] *Id.*

[64] *Id.* at 3.

[65] *Id.* at 3–5.

[66] *Id.* at 6–11.

[67] *Id.* at 5.

FERPA.[68] An additional white paper, *Amazon Web Services: Risk and Compliance*, is available for controllers seeking further understanding of AWS's reports, accreditations, and third-party reports.[69]

C. Azure (Microsoft)

Microsoft introduces Azure[70] on the Microsoft Trust Center as a platform that includes a "growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and web."[71] The company goes on to state:

> We understand that some organizations are still wary about cloud computing; keeping data confidential is essential for any organization. That's why Microsoft has made an industry-leading commitment to the protection and privacy of your data. We were the first cloud provider recognized by the European Union's data protection authorities for our commitment to rigorous EU privacy laws. Microsoft was also the first major cloud provider to adopt the new international cloud privacy standard, ISO 27018.[72]

The Azure section in the Trust Center includes five detailed sections: "Azure Compliance" (international, industry, and country specific standards); "Privacy" (data protection); "Transparency" (visibility to customer data); "Azure Government" (unique cloud instance for Governments); and "Azure Industries" (sector specific information).[73] There are two further sections dedicated to "Security" (Security Development Lifecycle [SDL]): "Active Directory" ([AD] and multi-factor authentication),[74] and "GDPR" (enabling compliance using Azure).[75] We will focus our evaluation on the final section.

1. Transparency

The Trust Center is a virtually unlimited collection of documentation related to compliance, security, and privacy, including a large section

[68] *Id.* at 12–13.

[69] *Id.* at 13.

[70] *Microsoft Azure*, MICROSOFT, https://www.microsoft.com/en-us/TrustCenter/CloudServices/Azure/default.aspx [https://perma.cc/5QTJ-G2GT]; *see also Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Azure*, MICROSOFT (Nov. 27, 2018), https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpia-azure#part-2—contents-of-a-dpia [https://perma.cc/H9DV-5WZ6].

[71] *Microsoft Azure*, *supra* note 70.

[72] *Id.*

[73] *Id.*

[74] *Microsoft Azure Security*, MICROSOFT, https://www.microsoft.com/en-us/TrustCenter/Security/azure-security [https://perma.cc/Z8P4-HP2S].

[75] *Microsoft Azure GDPR*, MICROSOFT, https://www.microsoft.com/en-us/TrustCenter/CloudServices/Azure/GDPR [https://perma.cc/W374-CJDS].

specific to GDPR requirements. As with other large technology companies, Microsoft offers multiple products and services across different geographies, some intended directly for individual consumers and others for businesses and partners. It can be challenging to navigate to and discover documentation that speaks specifically to Azure and the GDPR. For example, navigating to the Azure section yields a link to "GDPR," which provides six different options under four different categories that all link to another homepage of "Azure Security Documentation" or the "Azure Security Center."[76] However, on the same Azure homepage there is also an option for "Privacy" in the header that leads to three options: "Data Management," "GDPR," or "Resources." Following "GDPR" leads to six options, each of which take the user to a different page, some of which mention "Microsoft 365" or "Microsoft Cloud," and some of which mention no particular product at all.[77] Overall, there is a plethora of resources that link from the Trust Center (and a number of others available through other generic searching—e.g., "data tenancy" yields a number of documents that talk about data localization requirements under the GDPR). Generally, any user with sufficient time could find and review a number of documents that outline, with varying degrees of detail, the company's commitment to GDPR requirements. It would require a non-subject matter expert a number of hours to find the appropriately relevant documents (precise search versus general search and review time). However, these documents are available without registration or signing an NDA.[78]

2. Readability

No particular technical or legal background is necessary to review the documents; admittedly, the average person may not find their way to the Microsoft Trust Center as a casual observer. With a Flesch Reading Ease score of 21.1, and a Flesch-Kincaid readability score of 15.67, the general Azure GDPR documentation is definitely geared towards a highly educated or experienced reader. As expected, more specific documentation (a blog post, for example, on how to use Azure to streamline data subject requests as enabled by GDPR[79]) scores similarly to technical reading. The documents range from relatively short (around a thousand words), to moderately long (fifteen-page white papers, almost

[76] *Id.*

[77] *Microsoft Azure*, *supra* note 70.

[78] *Microsoft Documentation*, MICROSOFT, https://technet.microsoft.com/en-us/ms376608.aspx [https://perma.cc/64EY-B7GM].

[79] Tom Keane, *Streamlining GDPR Requests with the Azure Portal*, MICROSOFT (Apr. 16, 2018), https://azure.microsoft.com/en-us/blog/streamlining-gdpr-requests-with-the-azure-portal/ [https://perma.cc/ZD3Q-2XRK].

five thousand words[80]), to rather lengthy (forty-four pages, over twenty-three thousand words[81]) Online Services Terms (OST).

The OST covers a multitude of services, including some components of Azure, and it spells out Microsoft's commitment to compliance (along with its expectations of customers and users). In addition, the OST provides clauses noting where customers may obtain additional compliance related information, for example: "If Customer requests, Microsoft will provide Customer with each Microsoft Audit Report. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor."[82] There are an additional thirty-four service level agreements available on the "Microsoft Service Level Agreements" site, which contain additional limitations and commitments.[83]

3. Accountability

Microsoft expressly spells out the data processor and controller relationships in the Trust Center under the "European Union Model Clauses" page.[84] The company offers "Model Clauses" (also referred to as Standard Contractual Clauses) that outline the transfer of personal information for *in-scope* Microsoft services. More specifically, Microsoft notes:

> [E]nterprise customers, who are the controllers of the personal data, carry the primary obligation to protect that data. This means that European Economic Area (EEA) enterprise customers have a strong interest in ensuring that their service provider abides by EU data protection laws, or the customer can face liability—and even blockage of its ability to use a service.[85]

Interestingly, Microsoft is the only provider to have declared publicly the submission of its "Standard Contractual Clauses for review by the European Union's Article 29 Working Party," which authored the GDPR. The outcome of this review is stated by the company: "The group determined that implementation of the provisions in Microsoft agreements was in line with their stringent requirements." (Microsoft was the first cloud service provider to receive a letter of endorsement and approval

[80] *Online Services Terms (OST)*, MICROSOFT, https://www.microsoft.com/en-us/licensing/product-licensing/products [https://perma.cc/RX2D-3ADP].

[81] *Id.*

[82] *Id.* at 9.

[83] *Service Level Agreements*, MICROSOFT, https://azure.microsoft.com/en-us/support/legal/sla/ [https://perma.cc/S7MY-Q2XD].

[84] *European Union Model Clauses*, MICROSOFT, https://www.microsoft.com/enus/TrustCenter/Compliance/EU-Model-Clauses [https://perma.cc/QJ43-62N5].

[85] *Id.*

from the group.)[86] The "approval" covers the clauses but not the appendices of the service, where the details of specific data transfers and security measures are outlined.

One particular white paper, *Trusting the Cloud*, describes in greater detail (and equal measure) the privacy and security measures that Microsoft incorporates into the Azure services.[87] Without specifically mapping to the GDPR, this paper addresses the core requirements of logging, monitoring, access controls, lawful access, and data localization options. Overall, this is a relatively easy, understandable guide that gives the reader enough material to address the basic questions and also provides an introduction to some of the core related concepts.

D. Google Cloud Services

Google provides computing, storage, and database services[88] that comprise the Google Cloud Platform.[89] Each of these services is further broken down into a number of more detailed services. Additionally, Google provides various other services, such as identity and access management services, that can be integrated with and support its Google Cloud Platform.[90]

Privacy and security for Google Cloud Platform are discussed in "Trust & Security," which addresses "Infrastructure" (high-level description of the security components of its architecture), "Security Products" (solutions available to clients to support security), and "Transparency & Privacy" (high-level commitments to protecting privacy of its customers' data).[91] Additionally, the Trust & Security Page highlights the key security and privacy standards and legislation with which it is compliant, including the GDPR. Compliance with the GDPR is

[86] *Id.*

[87] *See generally* MICROSOFT, TRUSTING THE CLOUD (Nov. 2014), http://download.microsoft.com/download/5/C/7/5C770A50-4FE4-4052-98E1-562EBFE4F35A/Trusted_Cloud_White_paper_EN_US.pdf [https://perma.cc/BMC8-DQPM].

[88] *Google Cloud and the General Data Protection Regulation (GDPR)*, GOOGLE CLOUD, https://cloud.google.com/security/gdpr/ [https://perma.cc/MGR7-ZU8K]; *see also* GOOGLE CLOUD, GOOGLE CLOUD SECURITY AND COMPLIANCE WHITEPAPER: HOW GOOGLE PROTECTS YOUR DATA, https://static.googleusercontent.com/media/gsuite.google.com/en//files/google-apps-security-and-compliance-whitepaper.pdf [https://perma.cc/S29X-LXCS]; *Compliance*, GOOGLE CLOUD, https://support.google.com/googlecloud/answer/6056694?hl=en [https://perma.cc/7SSW-ZWJ8]; *Standards, Regulations & Certifications*, GOOGLE CLOUD, https://cloud.google.com/security/compliance/#/ [https://perma.cc/DA4B-Y8FC].

[89] For a description of Google Cloud Platform, see *Products and Services: Secure Your Data, Gain Real-Time Insights, Boost Productivity, and More*, GOOGLE CLOUD, https://cloud.google.com/products/ [https://perma.cc/6SF8-BWNY].

[90] *See id.*

[91] *Trust & Security*, GOOGLE CLOUD, https://cloud.google.com/security/ [https://perma.cc/SR4N-LVE3].

described more fully in the section "Google Cloud and the General Data Protection Regulation (GDPR)"[92] and the white paper *General Data Protection Regulation (GDPR)*.[93] This information is supported by another key white paper: *Google Cloud Security and Compliance Whitepaper: How Google Protects Your Data*.[94]

1. Transparency

Google makes publicly available a variety of high-level, highly detailed security and privacy information through its cloud computing website. The information relates to Google's commitment to privacy and security, the certifications that it maintains, and in some cases, its responses to privacy and security obligations. The information is made available without having to register or login.

With respect to the GDPR specifically, Google publishes its Terms of Service in full, which allows a prospective controller to evaluate whether the Terms of Service meet the controller's needs. Google additionally maps the Terms of Service against Article 28 of the GDPR,[95] which supports the controller in assessing to what extent Google commits to meeting its obligations under Article 28.

Google also provides high-level information on how it meets its obligations and commitments. The key focus of its documentation is publishing reports by independent auditors, which assert that Google is compliant with various standards (e.g., the SOC 3 report). More detailed reports, such as the SOC 2 compliance report, are only available with a nondisclosure agreement.[96] However, Google publishes on its website the white paper *Google Cloud Security and Compliance Whitepaper: How Google Protects Your Data*, which provides relatively detailed information about Google's privacy and security management practices to support a controller making an informed decision about whether it would be interested in engaging Google further.[97]

[92] *Google Cloud and the General Data Protection Regulation (GDPR)*, *supra* note 88.

[93] GOOGLE CLOUD, GENERAL DATA PROTECTION REGULATION (GDPR) (May 2018), https://cloud.google.com/security/gdpr/resource-center/pdf/googlecloud_gdpr_whitepaper_618.pdf [https://perma.cc/6N3N-KYKS].

[94] GOOGLE CLOUD SECURITY AND COMPLIANCE WHITEPAPER: HOW GOOGLE PROTECTS YOUR DATA, *supra* note 88.

[95] *Contracts & Terms*, GOOGLE CLOUD, https://cloud.google.com/security/gdpr/resource-center/contracts-and-terms [https://perma.cc/V7HX-SQDY].

[96] *Standards, Regulations & Certifications*, GOOGLE CLOUD, https://cloud.google.com/security/compliance/#/ [https://perma.cc/DA4B-Y8FC].

[97] GOOGLE CLOUD SECURITY AND COMPLIANCE WHITEPAPER: HOW GOOGLE PROTECTS YOUR DATA, *supra* note 88.

2. Readability

Finding the relevant privacy and security information on the Google website is sometimes challenging because some of the information is buried quite deep in the site, as of the writing of this Article. The Trust & Security section is relatively easy to find because the link appears right on the Google Cloud Platform page. From the Trust & Security section, the reader can navigate to information specifically on Google's security controls[98] and information on its compliance with the GDPR.[99] However, the information presented on those pages are high-level commitments to meeting their obligations. The reader must navigate to deeper level pages to find more detailed information on Google's approach to meeting its obligations.

Readability was assessed by generating the Flesch Reading Ease score and the Flesch-Kincaid Grade Level score on key pages describing Google's commitment and approach to meeting its privacy and security obligations. Google's page describing its commitment to meeting GDPR requirements[100] received a Flesch Reading Ease score of 21.3 and a Reading Grade Level score of 15.8. Google's page providing an overview of its approach to security management[101] received a Flesch Reading Ease score of 23.7 and a Flesch-Kincaid Grade Level score of 14.8. These scores reflect a reading level intended for university graduates and academics.[102] While it is difficult to establish the target reading level at which publicly available information should be written, these scores would likely exceed it.

3. Accountability

The page "Data Processing Terms"[103] outlines the terms and conditions under which Google processes data on behalf of its customers—i.e., the controllers. The terms apply to any customer on whose behalf Google processes data, including where subject to the GDPR. Paragraph 4.1 of Data Processing Terms discusses the applicability of the GDPR and indicates that the GDPR applies where the

[98] *Standards, Regulations & Certifications*, *supra* note 96.

[99] *Google Cloud and the General Data Protection Regulation (GDPR)*, *supra* note 88.

[100] *Id.*

[101] GOOGLE CLOUD, GOOGLE SECURITY WHITEPAPER (Jan. 2019), https://cloud.google.com/security/overview/whitepaper [https://perma.cc/C5YH-SMR5].

[102] Ruth Colmer, *The Flesch Reading Ease and Flesch-Kincaid Grade Level*, READABLE: BLOG, https://readable.io/blog/the-flesch-reading-ease-and-flesch-kincaid-grade-level/ [https://perma.cc/2748-6ZFV].

[103] *Data Processing and Security Terms (Customers)*, GOOGLE CLOUD, https://cloud.google.com/terms/data-processing-terms [https://perma.cc/6SA9-7GV9].

customer is in the European Union or where the customer offers services or monitors European citizens.

The terms also clearly establish and acknowledge the respective roles between Google and its customers. Paragraph 5.1.1 describes the relationship between Google and its customers. It acknowledges that the customer is the data controller[104] and that Google is the data processor. It then establishes the purposes for which Google is authorized to process data on behalf of the controller:

> 5.2.1 Customer's Instructions. By entering into these Terms, Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and TSS; (b) as further specified via Customer's use of the Services (including the Admin Console and other functionality of the Services) and TSS; (c) as documented in the form of the Agreement, including these Terms; and (d) as further documented in any other written instructions given by Customer and acknowledged by Google as constituting instructions for purposes of these Terms.[105]

The Data Processing Terms also describe the obligations that Google must meet in delivering its services. The obligations range from deploying technical safeguards, such as ensuring that appropriate information security safeguards are in place, to administrative controls, such as compelling Google to contractually obligate any sub-processors to meet the same terms.

E. Summary

Having examined each of the market leaders in turn, it becomes apparent that both AWS and Azure are transparent about their privacy practices. This is particularly true in their role as processor, rather than as controller. All three providers, however, have fairly robust language in their published documentation that does not easily lend itself to readability. Overall, without a fairly significant level of subject matter expertise, there is some guesswork involved in the interpretation and use of certain terms. Controllers, particularly those in a small- or medium-size organization, may not have the resources to fully examine and confirm that each of these larger processors have put in appropriate governance, processes, and technology to safeguard privacy.

[104] *Id.* The Data Processing Terms also acknowledges that the customer may be a processor, presumably where it is offering services to another party who is the controller. This relationship is not germane to this analysis and therefore not discussed here.

[105] *Id.*

IV. RISK

Using the obligations outlined in Part II and the processor information outlined in Part III, we seek to examine how a controller may assess risk.

Step 1: Assess

It follows that the traditional categories for risk analysis—impact, probability, and likelihood—are applicable here. However, for any organization using a cloud service, a data subject's data likely ends up in the hands of either Microsoft, Amazon, or Google as the top three cloud service providers, or in their partners or resellers hands. Risk calculations, therefore, can and should focus more on the inherent gap in the standard data flow of computing that is causing the risk to occur, as there is little that a controller, especially a small- or medium-size organization, may be able to do to change a processors' existing contracts or architecture.

Given that constraint, it appears there is little a controller can actually do to force a better compliance position with the processor. So, we turn instead to an examination of the specific risk at hand for all involved: non-compliance with the GDPR. Harms from non-compliance include three specific elements:

1. direct action by data subjects;
2. liability via controller; and
3. sanctions, including audits, investigations, and fines.

Despite the inability of controllers to change its processors' practices, it is incumbent upon controllers to protect its customers' data to the fullest extent before sending it to processors. Without recognizing this critical step, controllers expose themselves to GDPR-violation consequences.

Step 2: Manage and Mitigate

Although controllers have little control over the infrastructure their processors use, controllers' GDPR-imposed responsibility to ensure processors—here, cloud providers—comply with the Regulation principles remains. Controllers may choose to proactively design for privacy in an effort to send the least risk-prone data to processors. The key mechanism to mitigate risk is by encrypting personal information before or while it is transferred to the cloud provider's infrastructure without providing the cloud provider with the encryption key. Although this practice does not address all potential security issues that expose data, it is a foundational safeguard against unauthorized use of the data. However, this may only be possible where the cloud provider provides infrastructure-as-a-service rather than software-as-a-service because it likely controls the encryption key where it provides software-as-a-service.

In absence of encrypting the data prior to transferring it to the cloud provider, the controller should require the processor to implement administrative safeguards, such as:

- Restricting the processor from using the PI for its own purposes.
- Requiring the processor to ensure its own staff and contractors meet the same obligations.
- Having information handling policies and procedures in place.
- Having an industry-standard security program in place.
- Notifying the controller in the event of a security event resulting in unauthorized use or disclosure.
- Working with the controller to address privacy issues and notifying the controller where a request for the data is made.
- Providing audit results on a regularly scheduled basis.

Safeguards such as these help to lessen the chance that a controller's risk profile will be unnecessarily increased by the processor's practices.

CONCLUSION

A controller is accountable for protecting the privacy and personal information of the data subjects about whom it collects personal information. Where the controller uses a processor, the controller relies on the processor meeting its own contractual and statutory obligations to ensure that the controller's privacy posture is strong and is able to meet its requirement to protect data subjects' privacy and personal information. A processor failing to meet its obligation—by using personal information for unauthorized purposes or by failing to safeguard the personal information, for example—undermines the controller's ability to meet its obligations. The controller may still be held accountable despite not being responsible for the privacy issue.

A basic yet important safeguard in ensuring the processor is able to meet its obligations is simply reviewing the documentation that describes the privacy and security safeguards and information handling practices that the processor has in place. This includes not only legal documentation such as agreements but also internal documentation such as policies, procedures, white papers, and others. As noted in this Article, the three large cloud providers are generally quite transparent about how in their role as processors they support controllers in meeting their privacy obligations. The large cloud providers discussed in this Article provide a significant amount of information that supports a controller making an informed decision about whether their privacy practices are adequate.

But a key challenge for the privacy practitioner remains: Are the processor's privacy practices adequate? A processor may be transparent about their privacy practices—but are the disclosed practices effective? The privacy practitioner will need to make a risk-based decision about whether to engage a processor that has gaps in its privacy practices. The privacy practitioner must assess to what extent the gaps in the privacy practices will result in harm to the data subject. And privacy professionals must ask to what extent the gaps could increase legal, financial, or reputational risk for the controller, and whether engaging the processor is worth the risk.