International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 05 Issue 09 September 2022

DOI: 10.47191/ijsshr/v5-i9-14, Impact factor- 5.871

Page No: 4071-4082

How American Businesses Could Approach Trade with Companies in South America that Are Located in Adequate and Non-Adequate Countries

Donald L. Buresh, Ph.D., Esq.
Touro University Worldwide

ABSTRACT: This essay discusses the legal data privacy issues faced when doing business with a European Union (EU) member or a GDPR-compliant country that is not a member of the EU. The EU data transfer requirements are briefly explained, followed by a description of the South American nations that are General Data Protection Regulation (GDPR)-complaint or near GDPR-compliant, including Argentina, Brazil, Chile, and Uruguay. The paper talks about whether the United States or any of the states in the Union can be considered by the European Commission (EC) to be an adequate country and the impacts of the United States not being an adequate country. The former United States Privacy Shield (Shield) and its predecessor, the International Safe Harbor Privacy Principles (ISHPP), both of which were invalidated by the EC. Although the United States and the EU recently announced the Trans-Atlantic Data Privacy Framework (TADPF), the EC is anticipated to invalidate this framework. It is recommended that companies employ the pre-approved standard contractual clauses (SCCs) as the least risky endeavor to assure personal data privacy. The paper then turns to the issues involved in leveraging existing privacy policies. In this regard, the United States' sectoral approach to privacy is examined. The leverage issues that exist when interacting with GDPR-complaint countries are considered. Two lists of recommendations are presented, the first list being more general-purposes, while the second list is specific. The paper concludes by observing that a firm should analyze the privacy laws under which it is covered, select the most inclusive policies and procedures so that the company is compliant with the GDPR and state and federal sectoral laws, and implement the resulting conservative privacy framework.

KEYWORDS: Adequate Country, Data Transfer Requirements, European Commission, General Data Protection Regulation, Standard Contractual Clauses, United States Privacy Shield

Abbreviations:

The following abbreviations are used in this manuscript:

Abbreviation	Description
AI	Artificial Intelligence
AMEX	American Express
BAA	Business Associate Agreement
BIPA	Illinois Biometric Information Privacy Act
CCPA	California Consumer Privacy Act
CPRA	California Privacy Rights Act
COBIT	Control Objectives for Information and related Technology
CPO	Chief Privacy Officer
FedRAMP	Federal Risk and Authorization Program
FERPA	Family Educational Rights and Privacy Act
FFIEC	Federal Financial Institutions Examination council
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
IRS	Internal Revenue Service
IDS	Intrusion Detection System

IPS	Intrusion Prevention System
IT	Information Technology
ISACA	Information Systems Audit and Control Association
JCB	Japanese Credit Bureau
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number

INTRODUCTION

This essay highlights the legal data privacy issues faced when doing business with a European Union (EU) member or a GDPR-compliant country that is not a member of the EU. The EU data transfer requirements are briefly explained, followed by a description of the Latin American nations in South America that are General Data Protection Regulation (GDPR)-complaint or near GDPR-compliant, including Argentina, Brazil, Chile, and Uruguay. The next section discusses whether the United States or any of the states in the Union can be considered by the European Commission (EC) to be an adequate country and the impacts of the United States not being an adequate country.

The following section highlights the former United States Privacy Shield (Shield) and its predecessor, the International Safe Harbor Privacy Principles (ISHPP), both of which were invalidated by the EC. Although the United States and the EU recently announced the Trans-Atlantic Data Privacy Framework (TADPF), the EC is anticipated to invalidate this framework. It is recommended that companies employ the pre-approved standard contractual clauses (SCCs) as the least risky endeavor to assure personal data privacy.

The essay then turns to the issues involved in leveraging existing privacy policies. In this regard, the United States' sectoral approach to privacy is examined. The leverage issues that exist when interacting with GDPR-complaint countries are considered. Two lists of recommendations are presented, the first list being more general-purposes, while the second list is specific. The paper concludes by observing that a firm should analyze the privacy laws under which it is covered, select the most inclusive policies and procedures so that the company is compliant with the GDPR and state and federal sectoral laws, and implement the resulting conservative privacy framework.

European Union Data Transfer Requirements

The EU definition of an adequate country is explained in this section of the essay, and the differences between an adequate and inadequate country are described. According to the EC, a country is adequate if its laws securely protect personal data. Otherwise, the country is considered inadequate.

An adequate country is a country such that the European "Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of [] Article [45]."[1] In other words, an adequate country is "any country, territory or one or more specified sectors within that country, or organization that is located outside of the EEA and is recognized by the EC as ensuring an adequate level of protection of Personal Data."[2] An adequate country is a "country, territory, or specified sectors within a country and international organization published by the EC in the Official Journal of the EU for which it has decided that an adequate level of protection is ensured."[3]

When discussing the adequacy of a country, a country is adequate if the transfer of data to a country outside the EU is permitted. An adequate or secure nation is one "for which the [EC] has confirmed a suitable level of data protection based on an adequacy decision."[4] In adequate or secure countries, the EC has determined that the protection level for personal data is comparable under EU law.[5] The countries that currently provide adequate protection are Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, and Uruguay.[6] The EU expressly permits data transfers to these countries.

[1] *Art. 45 GDPR: Transfers on the Basis of an Adequacy Decision*, INTERSOFT CONSULTING (n.d.), *available at* https://gdpr-info.eu/art-45-gdpr/.
[2] *Adequate Country Definition*, LAW INSIDER (n.d.), *available at* https://www.lawinsider.com/dictionary/adequate-country.
[3] *Id.*
[4] *GDPR: Third Countries*, INTERSOFT CONSULTING (n.d.), *available at* https://gdpr-info.eu/issues/third-countries/.
[5] *Id.*
[6] *Id.*

How American Businesses Could Approach Trade with Companies in South America that Are Located in Adequate and Non-Adequate Countries

The presumption is that any country that has not yet been confirmed to protect personal data adequately is inadequate. The United States has not yet been confirmed to be an adequate country because it does not possess a federal privacy law that adequately protects personal data.[7]

Privacy Regimes in Latin America

The four Latin American countries with personal data privacy regimes are Argentina, Brazil, Chile, and Uruguay. Argentina and Uruguay have been classified by the EC as adequate countries, meaning that their data privacy laws are sufficient to assure the privacy of personal data when the data of EU data subjects are transferred to these two nations. Although Chile enacted a data privacy law in 1999, long before the GDPR was enacted in 2016, the law does not adequately protect personal data transfers, according to the EC. Finally, in 2021, Brazil GDPR-like law in 2020. Unfortunately, the law is too new, and the EC has yet to rule on whether Brazil is an adequate country capable of securing the personal data of EU citizens. Each one of the laws will be briefly outlined in turn.

Data Privacy Law of Argentina

In Argentina, the Personal Data Protection Act 25.326 (PDPA) (*Ley de Protección de los Datos Personales*) was passed in 2000 to help protect the privacy of personal data by providing individuals access to any information stored in public and private databases and registries.[8] The Argentine Agency of Access to Public Information (*Agencia de Acceso a la Información Pública*, AAPI) within the Chief of Ministries' Cabinet is responsible for enforcing the PDPA.[9] The PDPA is aligned with the GDPR, and Argentina was the first country in Latin America to be deemed an adequate country for data transfers from the EC.[10] In 2016, the AAPI issued a new regulation, Provision 60-E/2016, that governed international transfers of personal data.[11] Under the rule, Argentina approved a model form that was partially based on the data transfer model in the GDPR for personal data transfers to data controllers and data processors.[12]

The problem with the PDPA is enforceability. According to Frene, from 2018 to 2021m the AAPI levied less than ten fines per year for PDPA infringement.[13] In all the cases, the fines did not exceed $2,000.[14] This fact demonstrates that the PDPA may not be an enforceable law. If a firm encounters a low probability of receiving a fine of approximately $1,000 for violating the PDPA, where is the incentive to comply with it? A company can merely pay the fine and treat it as the cost of doing business.[15] This may be good news for the company because if data privacy violations occur while personal data are located in Argentina, and data privacy is violated, the cost to the company is likely to be small. The benefit of transferring personal data to Argentina is that when a personal data violation occurs, the minuscule fines make it seem like personal data are being transferred to a non-EU-compliant nation. The company receives the benefit of a poor enforcement regime and the benefit that Argentina is an EC-determined adequate country.

Data Privacy Law of Brazil

The *Lei Geral de Proteção de Dados*, or General Data Protection Law (LGPD), is Brazil's legal framework to regulate the collection and use of personal data. The LGPD was passed on August 14, 2018,[16] and became effective on August 16, 2020.[17] The LGPD is enforced by the *Autoridade Nacional de Proteção de Dados* or the National Data Protection Authority (ANPD).[18] Although not the first data privacy law in South America, the LGPD is well publicized and is heavily influenced by the GDPR. The LGPD

---

[7] Donald L. Buresh, *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, 38 SANTA CLARA HIGH TECHNOLOGY LAW JOURNAL 1, 39-93 (Oct. 2021), https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2/.
[8] *Argentina Personal Data Protection Act (PDPA)*, MICROSOFT CORP. (Apr. 19, 2022), *available at* https://docs.microsoft.com/en-us/compliance/regulatory/offering-pdpa-argentina.
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] Lisandro Frene, *20 years of Argentinian Privacy Law: Its Current Status and What to Expect*, INTERNATIONAL BAR ASSOCIATION (Jun. 24, 2021), available at https://www.ibanet.org/twenty-years-of-Argentinian-privacy-law.
[14] *Id.*
[15] *Id.*
[16] *Brazil - Data Protection Overview*, DATA GUIDANCE (Mar.3, 2020), *available at* https://www.dataguidance.com/video/brazil-overview.
[17] *Brazil's General Data Protection Law / Lei Geral de Proteção de Dados (LGPD) – An Overview*, USERCENTRICS (Mar. 14, 2022), *available at* https://usercentrics.com/knowledge-hub/brazil-lgpd-general-data-protection-law-overview/#:~:text=The%20General%20Data%20Protection%20Law,effect%20on%20August%2016%2C%202020.
[18] *Id.*

expanded its privacy coverage from the GDPR's parameters.[19] The LGPD became effective for data subjects on September 18, 2020, and penalties became enforceable on August 1, 2021.[20]

Article 6 states that the LGPD principles governing data processing are purpose, adequacy, need, free access, data quality, transparency, security, prevention, non-discrimination, responsibility, and accountability.[21] The financial penalty for violating the LGPD is at most two percent of sales before taxes, or R$50 million, approximately €8 million.[22]

Unfortunately for the company, Brazil has yet to be approved by the EC as an adequate country. The reason is likely because of the newness of the law. The EC may be waiting to find out whether the law will be vigorously enforced or is a sham law with no teeth because Brazilian officials do not enforce it. The Brazilian data privacy law has great promise because it was modeled after the GDPR. For the company, this means that Brazil may be given adequate country status in the future.

` Provided that the firm is GDPR compliant, transferring personal data back and forth from Portugal to Brazil should be relatively easy. Another advantage of transferring personal data back and forth from Portugal to Brazil is that both speak Portuguese, whereas all other Latin American countries speak Spanish. This fact ensures no translation problems when business is conducted between Portugal and Brazil.

Data Privacy Law of Chile

In 1999, Chile enacted its first regulation on data privacy, Law No. 19.628/1999, 'On the protection of private life,' commonly referred to as Personal Data Protection Law (PDPL).[23] The PDPL defines and regulates the processing of personal data that is not governed by the various Chilean sectoral laws.[24] The PDPL states that personal data may only be processed if the processing is permitted by law or based on the data subject's prior informed, written consent.[25] The exception to the PDPL includes specific publicly accessible data or internal data processing only.[26] The PDPL also contains special regulations regarding economic, banking, and financial obligations.[27] The data subject's rights listed in the PDPL include the right to access, rectify, delete, block, and object to processing personal data in some instances.[28]

However, although the PDPL was the first data privacy law in Latin America, the law quickly became immaterial because there was practically no enforcement, owing to no cataloging violations, no official data privacy authority, low fines, and other flaws in the law.[29] This fact is not beneficial to the company when personal data is being transferred from Portugal, a member of the EU, and Chile. Because Chile is not an adequate country as determined by the EC, it is in the firm's best interest not to transfer the personal data of EU data subjects to Chile. To do so would run afoul of the GDPR, thereby probably incurring legal liability under the GDPR.

Data Privacy Law of Uruguay

In August 2008, Uruguay enacted Law No. 18.331 on the Protection of Personal Data and Habeas Data Action (PPD-HAD) and Decree No. 414/009 Regulating Law 18.331.[30] For years, Uruguay has shown its preference for the GDPR.[31] In August 2012, the EC decided to recognize Uruguay as ensuring an adequate level of protection within Article 25(6) of Directive 95/46/EC of the European Parliament and the Council of Europe.[32] Uruguay was the first non-European nation to follow Convention 108 of the European Council, recently including the Convention's amendments in furtherance of its compliance with the GDPR's

[19] *Id.*
[20] *Brazil – Data Protection Overview*, *supra*, note 39,
[21] *Id.*
[22] *Id.*
[23] *Chile's Personal Data Protection Law*, DATA PROTECTION LAWS OF THE WORLD (Jan. 24, 2022), *available at* https://www.dlapiperdataprotection.com/index.html?t=law&c=CL#:~:text=19%20N°%204,of%20his%2Fher%20personal%20data.
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] Macarena Gatica, *Chile - Data Protection Overview*, DATA GUIDANCE (Nov. 2021), *available at* https://www.dataguidance.com/notes/chile-data-protection-overview.
[30] Mariela Ruanova, *GDPR Three Years Later - Data Protection Legal framework in Uruguay*, DENTONS (n.d.), *available at* https://www.dentons.com/en/insights/articles/2021/may/10/gdpr-three-years-later-data-protection-legal-framework-in-uruguay.
[31] *Id.*
[32] *Id.*

regulations on data protection.[33] When the EU passed the GDPR in 2016, Uruguay enacted Law 19.670, which had provisions relating to data protection, addressing the "proactive responsibility" principle that supports the implementation of appropriate technical and organizational measures such as privacy by design and privacy by default, the obligation to designate a Data Protection Officer, and the rule of data breach notifications.[34] These provisions were further clarified by the regulatory Decree 64/020, which regulates the implementation and enforcement of these provisions.[35] In a joint effort, the Argentinian and Uruguayan data protection authorities approved the Guide on Data Protection Impact Assessments (DPIA Guide).[36]

`Presuming that the firm is GDPR-compliant, data transfers of personal data between Portugal and Uruguay are likely to occur without incident. The only issue with transferring back and forth from Portugal to Uruguay is that Uruguay is a Spanish-speaking country, which means that communications between the nations would have to be translated from Portuguese to Spanish and vice versa is a cost to the firm. With translation, there is a risk that personal information could be mistranslated, thereby potentially technically violating the GDPR. Even so, if the personal data is expressed in a commonly accepted European language, such as English or French, this issue may not be as severe as initially thought.

Is the United States an Adequate Country?

Is it appropriate for the EU could consider the United States an adequate country because the states of California, Colorado, Connecticut, Utah, and Virginia have comprehensive privacy laws? The short answer is no. The reason is that California, Colorado, Connecticut, Utah, and Virginia are states inside the United States. Through the United States Constitution, these states have ceded enumerated sovereign power to the United States federal government. For example, states in the United States have ceded their sovereign power to negotiate with other nations and make war on other countries. The complete list of ceded powers is contained in the Constitution.

A state within the United States is not a territory, where territory is a "geographical area belonging to or under the jurisdiction of a governmental authority."[37] The difference between a state and a territory is that territory is an area "under the control of another state or government and does not have sovereignty, while a state is also known as a country or an organized political organization that enjoys sovereignty."[38]

A state in the United States is not a sector within the United States. According to Kenton, a sector is an "area of the economy in which businesses share the same or related business activity, product, or service."[39] A sector is a large grouping of companies with similar business activities.[40] For example, car manufacturers or computer manufacturers constitute a sector. A state is not a sector because states contain companies with various business activities, not a single business activity or similar business activities. Thus, a state is not a sector.

A state within the United States is not an international organization. As explicitly stated in the United States Constitution, a state cannot negotiate with foreign nations.[41] There is nothing international about a state in the United States. A state within the United States is a governmental body, not an international non-government organization. Thus a state is not an international organization.

Could the EC recognize California, Colorado, Connecticut, Utah, or Virginia as adequate states? The answer is maybe. However, in affirming these five states to be adequate states, the EC would have to find that once EU personal data are transferred from the EU to one or more of these states, the data are adequately protected. Another issue that the EC would likely consider is the protection status of EU personal data as it moves inside the United States from an adequate state to an inadequate state or one or more of the 45 states that have yet to pass a comprehensive privacy law. If the transfer of EU personal data is insecure when it arrives inside an insecure state, the EC would likely either disapprove of the data transfer or not permit EU personal data to be transferred to any state inside the United States. The reason is that one inadequate state is sufficient to thwart data security. In

---

[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] Ana Brian Nougrères, *Uruguay - Data Protection Overview*, DATA GUIDANCE (Mar. 2022), *available at* https://www.dataguidance.com/notes/uruguay-data-protection-overview#.
[37] *Territory*, MERRIAM-WEBSTER DICTIONARY (n.d.), *available at* https://www.merriam-webster.com/dictionary/territory#:~:text=Legal%20Definition%20of%20territory,political%20subdivision%20of%20a%20country.
[38] Emelda M., *Difference Between Territory and State*, DIFFERENCEBETWEEN.NET (n.d.), *available at* http://www.differencebetween.net/miscellaneous/politics/political-institutions/difference-between-territory-and-state/#:~:text=Summary%3A,political%20organization%20which%20enjoys%20sovereignty.
[39] Will Kenton, *Sector*, INVESTOPEDIA (May 28, 2022), *available at* https://www.investopedia.com/terms/s/sector.asp.
[40] *Id.*
[41] U.S. Const., Art. I, Sec. 10.

essence, a chain is only as strong as its weakest link, and a state that has yet to pass a comprehensive privacy law would be that weakest link.

The final possibility is that the EC could view the United States as an adequate country because at least one state, for example, California, protects personal data adequately. This theory commits the logical fallacy of composition or hasty generalization, where what is valid for a part of something must also be true for the whole.[42] This argument suffers from the same problem as the previous argument. If EU personal data is transferred to a state that has not yet passed a comprehensive privacy law acceptable to the EU, the EC would likely consider the data unnecessarily being exposed to risk.

Therefore, under no circumstance is the EC likely to determine that the United States is an adequate country, even if at least one state has passed an acceptable privacy law. The United States needs to pass a comprehensive federal privacy law to be considered by the EC as an adequate country.

Impacts of the United States Not Being an Adequate Country

There are two impacts of the United States not being an adequate country. The first impact is national security, while the second is economic. The national security impact is that the United States may not be able to obtain data on threat actors that reside in the EU because of privacy considerations. The issue is data localization, where data localization keeps data in its origin region.[43] Data residency refers to where the data is stored.[44] The issue arises when threat actors reside in a country with strict data localization laws.[45] In this instance, the United States may have determined that a threat actor living in the EU is a person of interest based on Internet activities. With data localization, unless there are treaties overriding the GDPR and effective mechanisms, the EC may prevent a threat actor's data from being sent to the United States under the pretext of data privacy, thereby increasing the potency of the threat. From the perspective of the United States federal government, this is an unacceptable situation.

Another impact facing the United States from not being an adequate country is economic. Because America has not yet been classified as an adequate country, this fact may dampen trade between the United States and the EU. One way around the classification is to have trade relations with countries inside the EU that are independent of the GDPR. For example, the United States could develop trade relations with France that have nothing to do with the GDPR. Then, the GDPR cannot act as a barrier to trade with the United States.

Trans-Border Sharing of Personal Data

In this section, the former United States Privacy Shield (Shield) is discussed, observing that the EC invalidated the Shield because it failed to adequately protect EU citizens' personal data. The section briefly mentions that ISHPP was also invalidated before the Shield came into effect. The section points out that the United States and the EU recently announced a third data transfer framework, the Trans-Atlantic Data Privacy Framework (TADPF). It is projected that TADPF will also be invalidated by the EC, whereas the privacy approach with the least risk is to employ the GDPR pre-approved standard contractual clauses (SCCs).

The United States Privacy Shield

The Shield was a legal framework for regulating the exchange of personal data for business purposes between the EU and the United States.[46] One of Shield's purposes was to permit American firms to quickly receive personal data from EU members under EU privacy law that protected EU citizens.[47] The Shield became effective on July 12, 2016, when the EC approved it. It replaced ISHPP, which was declared invalid by the ECJ in October 2015.[48] The ISHPP is also known as Schrems I.[49]

---

[42] Brian Carlson, *30 Common Logical Fallacies–A Study Starter*, ACADEMIC INFLUENCE (Jul. 23, 2021), *available at* https://academicinfluence.com/inflection/study-guides/logical-fallacies.
[43] *What is Data Localization?*, CLOUDFLARE (n.d.), *available at* https://www.cloudflare.com/learning/privacy/what-is-data-localization/.
[44] *Id.*
[45] Erol Yayboke, Caroline G. Ramos, & Lindsey R. Sheppard, *The Real National Security Concerns over Data Localization*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (Jul. 23, 2021), *available at* https://www.csis.org/analysis/real-national-security-concerns-over-data-localization.
[46] *EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield*, EUROPEAN COMMISSION (Feb. 2, 2016), *available at* https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216.
[47] E. L., *The New Trnsatlantic Data "Privacy Shield"*, THE ECONOMIST (Feb. 2, 2016), *available at* https://www.economist.com/the-economist-explains/2016/02/02/the-new-transatlantic-data-privacy-shield.
[48] *Commissioner Jourová's Remarks on Safe Harbour EU Court of Justice Judgement before the Committee on Civil Liberties, Justice and Home Affairs (Libe)*, EUROPEAN COMMISSION (Oct. 26, 2015), *available at* https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_15_5916.
[49] *Id.*

How American Businesses Could Approach Trade with Companies in South America that Are Located in Adequate and Non-Adequate Countries

At its onset, the Shield was destined for failure. Article 29 Data Protection Working Party opined on April 13, 2016, that the Shield improved on the ISHPP, but there remained issues with data deletion, collection of massive amounts of data, and the role of the Ombudsperson.[50]The European Data Protection Supervisor observed on May 30, 2016, that the Shield was insufficiently robust to withstand legal scrutiny.[51] On July 8, 2016, the Article 31 committee approved the Shield's final version; on July 12, 2016, the EC approved the Shield.[52] On January 25, 2017, President Donald Trump signed an executive order entitled *Enhancing Public Safety*, stating that the United States privacy protections would not be extended beyond American citizens or residents.[53] President Joseph Biden repealed this executive order on January 20, 2021.[54]

In invalidating the Shield, the EC stated that:

"The US Privacy Act has never offered data protection rights to Europeans. The Commission negotiated two additional instruments to ensure that EU citizens' data is duly protected when transferred to the US:

- The EU–US Privacy Shield, which does not rely on the protections under the US Privacy Act.
- The EU–US Umbrella Agreement, which enters into force on February 1 (2017). To finalize this agreement, the US Congress adopted a new law in 2017, the US Judicial Redress Act,[55] which extends the benefits of the US Privacy Act to Europeans and gives them access to US courts."[56]

The ECJ declared the Shield invalid on July 16, 2020, in the case known as Schrems II.[57] In 2022, the United States and the EU announced that a new data transfer framework entitled the Trans-Atlantic Data Privacy Framework (TADPF) had been agreed upon, replacing the Shield.[58]

Standard Contractual Clauses

Given that the ISHPP and Shield were both declared invalid by the ECJ, it does not make sense to rely on the TADPF. To do so is probably a high risk. A better alternative is to rely on the GDPR standard contractual clauses (SCCs) and incorporate these clauses into future contracts with European entities.

The GDPR clauses were modernized on June 4, 2021, and reflect the appropriate data protection safeguards when data are transferred from the EU to non-EU countries.[59] The SCCs have been pre-approved by the EC.[60] The updated clauses replaced the three sets of SCCs that were adopted under the Data Protection Directive 95/46. As of September 27, 2021, it is impossible to enter into contracts incorporating these earlier SCCs.[61] Until December 27, 2022, data controllers and processes may rely on these earlier SCCs for contracts signed before September 27, 2021, assuming that the processing operations do not change.[62] The EC created Questions and Answers (Q&As) to give practical suggestions on using the new SCCs and help stakeholders comply with the

---

[50] *Article 29 working party archives 1997 – 2016*, EUROPEAN COMMISSION (2016), *available at* https://ec.europa.eu/justice/article-29/documentation/index_en.htm.

[51] *Privacy Shield: More Robust and Sustainable Solution Needed*, EUROPEAN DATA PROTECTION SUPERVISOR (May 30, 2016), *available at* https://web.archive.org/web/20160625142411/https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf.

[52] European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows, EUROPEAN COMMISSION (Jul. 12, 2016), *available at* https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461.

[53] Donald J. Trump, *Executive Order: Enhancing Public Safety in the Interior of the United States*, THE WHITE HOURS (Jan. 25, 2017), *available at* https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/.

[54] Joseph R. Biden, *Executive Order on the Revision of Civil Immigration Enforcement Policies and Priorities*, THE WHITE HOURS (Jan. 20, 2021), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-the-revision-of-civil-immigration-enforcement-policies-and-priorities/.

[55] Pub. L. 114-126, JUDICIAL REDRESS ACT OF 2015 (2015), *available at* https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf.

[56] Phil Muncaster, *Trump Order Sparks Privacy Shield Fears*, INFO SECURITY (Jan. 27, 2017), *available at* https://www.infosecurity-magazine.com/news/trump-order-sparks-privacy-shield/

[57] *EU-US Privacy Shield for Data Struck Down by Court*, BBC NEWS (Jul. 16, 2020), *available at* https://www.bbc.com/news/technology-53418898.

[58] David McCabe, & Martina Stevis Grindal, *U.S. and European Leaders Reach Deal on Trans-Atlantic Data Privacy*, THE NEW YORK TIMES (Mar. 25, 2022), *available at* https://www.nytimes.com/2022/03/25/business/us-europe-data-privacy.html.

[59] Standard Contractual Clauses (SCC), EUROPEAN COMMISSION (Jun. 4, 2021), *available at* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[60] *Id.*

[61] *Id.*

[62] *Id.*

GDPR.[63] The Q&As were based on feedback from various stakeholders regarding their experience in employing the new SCCs when they were first adopted.[64] The EC intends the Q&As to be a dynamic source of information and will probably be updated as the need arises.[65]

Recommendations for the Company

Based on the fact the ECJ invalidated the Shield on July 16, 2020, it does not make sense to recommend Shield to any global company. It also does not make sense to comply with the TADPF because if its two predecessors were found to be invalid, there is a significant probability that it, too, will be deemed invalid by the ECJ. A far better and legally safer alternative is incorporating the SCCs into future contracts with European entities, particularly between Portugal and other Latin American countries such as Brazil. The SCCs were pre-approved by the EC, and thus there is a negligible probability that they will be invalidated.

Leveraging Established Privacy Policies

In this section, the United States' sectoral approach to privacy is discussed. It also describes the data privacy issues that an American company faces when conducting business with public and private economic organizations in the EU. The section concludes by addressing the data privacy leverage issues in GDPR-compliant countries that are not EU members.

United States Sectoral Approach to Privacy

When one examines various federal privacy laws, one sees a hodge-podge. Some federal privacy laws adhere to all Fair Information Privacy and Practices (FIPP) principles, whereas other federal laws do not.[66] [67] [68] The federal privacy laws may not expressly state that they comply with a given FIPP principle. For example, the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, uses the (1) Privacy Rule and (2) Safeguard Rule.[69] The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA), possesses the Red Flag Rules.

The Health Insurance Portability and Accountability Act (HIPAA) possesses the following five rules: (1) Privacy Rule, (2) Transactions and Code Sets Rule, (3) Security Rule, (4) Unique Identifiers Rule, and (5) Enforcement Rule.[70] The Health Information Technology for Economic and Clinical Health Act (HITECH) also has a privacy and security rule but addresses the electronic transmission of health information.[71] In contrast, the Family Educational Rights and Privacy Act (FERPA) possesses privacy rules but no expressed security rules.[72] The same is true for the Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act. CAN-SPAM enjoys a privacy rule, but a specific security rule is conspicuous by its absence.[73]

As can be readily seen, there is only some consistency among the federal sectoral privacy laws. The laws do not explicitly adhere to the FIPPs guidelines and sometimes employ different terminology. From a business perspective, this byzantine legal framework leaves corporations in a quandary. Companies must be rather careful to comply with the appropriate sectoral law while simultaneously ensuring that it does not violate some other sectoral law. Although this situation does legal work for attorneys, it is not in society's best interest because it is not an efficient solution to the privacy problem.

---

[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] The Organisation for Economic Co-operation and Development (OECD) has codified the Fair Information Privacy Practices (FIPPs) guidelines into the following eight principles: (1)Collection Limitation Principle; (2) Data Quality Principle; (3) Purpose Specification Principle; (4) Use Limitation Principle; (5) Security Safeguards Principle; (6) Openness Principle; (7) Individual Participation Principle; and (8) Accountability Principle
[67] Tech Target Staff, *Fair Information Practices (FIP)*, TECH TARGET (Mar, 2011), *available at* https://www.techtarget.com/whatis/definition/Fair-Information-Practices-FIP.
[68] OECD Staff, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (n.d.), *available at* https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
[69] Garry Kranz, *Gramm-Leach-Bliley Act (GLBA)*, TECH TARGET (Jun. 2021), *available at* https://www.techtarget.com/searchcio/definition/Gramm-Leach-Bliley-Act.
[70] Peter F. Edemekong, Pavan Annamaraju, & Micelle J. Haydel, *Health Insurance Portability and Accountability Act*, NATIONAL LIBRARY OF MEDICINE (n.d.), available at https://www.ncbi.nlm.nih.gov/books/NBK500019/.
[71] HHS Staff, *HITECH Act Enforcement Interim Final Rule*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (Jun. 16, 20917), *available at* https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.
[72] DOE Staff, *Family Educational Rights and Privacy Act (FERPA)*, U.S. DEPARTMENT OF EDUCATION (Aug. 25, 2021), *available at* https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
[73] FTC Staff, CAN-SPAM Act: A Compliance Guide for Business, Federal Trade Commission (Jan. 2022), available at https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business.

Leverage Issues when Dealing with GDPR-Compliant Countries

Extreme care must be taken to bridge the chasm between the sectoral and comprehensive approaches to privacy, such as in the GDPR. First and foremost, consistent definitions must be specified that do not contradict the current definitions that are contained in the current sectoral laws. This is no mean feat because it resembles the fifth labor of Hercules, where the ancient Greek hero cleaned the Augean stables. Second, the scope of the GDPR should be well understood. The problem is that Congress has taken a sectoral approach for political reasons. The Constitution does not expressly state that American citizens have a fundamental right to privacy. Currently, all Americans possess a reasonable expectation of privacy, which Justice Harlan expressed in his concurrence in *Katz*.[74]

Thus, in leveraging established policies drafted for compliance with United States privacy policies and the GDPR, the risk-averse behavior dictates that the company employ a conservative approach regarding transferring personal data from and to Latin American countries and EU members. As long as the implemented security framework does not violate American privacy laws and is GDPR-compliant, the firm should be able to leverage its existing privacy policies with the GDPR. Suppose the company's privacy policies are inconsistent with the GDPR or violate American privacy law. In that case, every effort should be made to bring the company into compliance to avoid unnecessary litigation.

Recommendations for Compliance

A good security framework that is GDPR-acceptable is essential. From an overall perspective, the firm should:

- Have an overall compliance strategy;
- Have compliance subject-matter experts on staff or on a consulting basis;
- Inventory and assess personally identifiable information or sensitive personal information;
- Establish data protection policies and procedures that are consistent with the GDPR, various state privacy laws (e.g., California Consumer Privacy Act, etc.), and sectoral privacy laws;
- Develop an effective response strategy and plan;
- Maintain proper compliance documentation; and
- Guarantee proof of compliance.[75]

From a more concrete approach to data privacy, Mello compiled the following list of five recommendations for data protection compliance, including:

- Identify personal information that is created, received, and shared with other individuals and entities;
- Secure personal data across the enterprise among corporate suppliers and vendors against data breaches and inadvertent disclosure;
- Establish a legally compliant system to respond to requests by individuals for personal data about them that the company possesses;
- Produce a legally compliant process for producing reports on personal data that is in an easily recognizable format; and
- Create and maintain a legally compliant process to delete personal data when its storage no longer serves the purpose for which it was collected or upon request by the data subject which is affiliated with the personal data in question.[76]

In essence, the company should catalog the privacy laws covering its operations nationally and internationally and then adhere to the most stringent rules among the group of laws under consideration. This is no mean feat. Since security compliance is not necessarily a revenue generator but can be,[77] [78] a balance must be struck between business behavior that maximizes profits or equivalently minimizes costs[79] and data security compliance. The scales should probably be tipped towards data security compliance. Suppose personal data security is an issue worthy of corporate attention. In that case, the reduced expenses caused by

[74] *United States v. Katz*, 389 U.S. 347, 388 (1967).
[75] *Understanding Data Privacy: A Compliance Strategy Can Mitigate Cyber Threats*, THOMPSON REUTERS (n.d.), *available at* https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-a-compliance-strategy-can-mitigate-cyber-threats.
[76] John P. Mello, *5 Keys to Data Protection Compliance*, TECHBEACON (n.d.), *available at* https://techbeacon.com/security/go-beyond-policy-5-keys-data-protection-compliance.
[77] Jay Rosen, *How to Reposition Compliance as a Revenue Generator*, CORPORATE COMPLIANCE INSIGHTS (Apr. 18, 2019), *available at* https://www.corporatecomplianceinsights.com/how-to-reposition-compliance-as-a-revenue-generator/.
[78] Drayton Mayers, *Strong Cybersecurity Can Be a Revenue Generator – Here Is Why and How*, MEMPHIS BUSINESS JOURNAL (May 20, 2020), *available at* https://www.bizjournals.com/memphis/news/2020/05/20/strong-cybersecurity-can-be-a-revenue-generator.html.
[79] PAUL KRUGMAN, & ROBIN WELLS, ECONOMICS (Worth Publishers 6th ed. 2021).

successful compliance leading to a shortage of litigation is not only possible but also quite likely. The above recommendations should be taken to heart so that a firm can be simultaneously profitable and compliant.

CONCLUSION

The legal privacy trends in the United States, Europe, and other nations indicate that a comprehensive approach by the firm to privacy is critical. On an ever-increasing scale, nations are enacting wide-ranging privacy laws that are modeled after the GDPR. As GDPR compliance becomes an omnipresent feature of business behavior, compliance takes on a more demanding role in assuring profitability. Thus, company conduct regarding its processing of personal data becomes increasingly paramount with each passing day. The inevitable conclusion is that the firm should analyze the privacy laws under which it is covered and select the most inclusive policies and procedures that so that the company is compliant with the GDPR, as well as state and sectoral privacy laws, implementing a conservative privacy framework. Nothing less will suffice.

MISCELLANEOUS CONSIDERATIONS

Author Contributions: The author has read and agreed to the published version of the manuscript.
Funding: This research received no external funding.
Institutional Review Board Statement: Not applicable.
Informed Consent Statement: Not applicable.
Conflicts of Interest: The author declares no conflict of interest.
Acknowledgments: I acknowledge the insights on global privacy law that I received from Prof. Amy Apostol.

REFERENCES

1) Art. 45 GDPR: Transfers on the Basis of an Adequacy Decision, INTERSOFT CONSULTING (n.d.), available at https://gdpr-info.eu/art-45-gdpr/.
2) Adequate Country Definition, LAW INSIDER (n.d.), available at https://www.lawinsider.com/dictionary/adequate-country.
3) GDPR: Third Countries, INTERSOFT CONSULTING (n.d.), available at https://gdpr-info.eu/issues/third-countries/.
4) Donald L. Buresh, Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?, 38 SANTA CLARA HIGH TECHNOLOGY LAW JOURNAL 1, 39-93 (Oct. 2021), https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2/.
5) Argentina Personal Data Protection Act (PDPA), MICROSOFT CORP. (Apr. 19, 2022), available at https://docs.microsoft.com/en-us/compliance/regulatory/offering-pdpa-argentina.
6) Lisandro Frene, 20 years of Argentinian Privacy Law: Its Current Status and What to Expect, INTERNATIONAL BAR ASSOCIATION (Jun. 24, 2021), available at https://www.ibanet.org/twenty-years-of-Argentinian-privacy-law.
7) Brazil - Data Protection Overview, DATA GUIDANCE (Mar.3, 2020), available at https://www.dataguidance.com/video/brazil-overview.
8) Brazil's General Data Protection Law / Lei Geral de Proteção de Dados (LGPD) – An Overview, USERCENTRICS (Mar. 14, 2022), available at https://usercentrics.com/knowledge-hub/brazil-lgpd-general-data-protection-law-overview/#:~:text=The%20General%20Data%20Protection%20Law,effect%20on%20August%2016%2C%202020.
9) Brazil – Data Protection Overview, supra, note 39,
10) Chile's Personal Data Protection Law, DATA PROTECTION LAWS OF THE WORLD (Jan. 24, 2022), available at https://www.dlapiperdataprotection.com/index.html?t=law&c=CL#:~:text=19%20N°%204,of%20his%2Fher%20personal%20data.
11) Macarena Gatica, Chile - Data Protection Overview, DATA GUIDANCE (Nov. 2021), available at https://www.dataguidance.com/notes/chile-data-protection-overview.
12) Mariela Ruanova, GDPR Three Years Later - Data Protection Legal framework in Uruguay, DENTONS (n.d.), available at https://www.dentons.com/en/insights/articles/2021/may/10/gdpr-three-years-later-data-protection-legal-framework-in-uruguay.
13) Ana Brian Nougrères, Uruguay - Data Protection Overview, DATA GUIDANCE (Mar. 2022), available at https://www.dataguidance.com/notes/uruguay-data-protection-overview#.
14) Territory, MERRIAM-WEBSTER DICTIONARY (n.d.), available at https://www.merriam-webster.com/dictionary/territory#:~:text=Legal%20Definition%20of%20territory,political%20subdivision%20of%20a%20country.

15) Emelda M., Difference Between Territory and State, DIFFERENCEBETWEEN.NET (n.d.), available at http://www.differencebetween.net/miscellaneous/politics/political-institutions/difference-between-territory-and-state/#:~:text=Summary%3A,political%20organization%20which%20enjoys%20sovereignty.
16) Will Kenton, Sector, INVESTOPEDIA (May 28, 2022), available at https://www.investopedia.com/terms/s/sector.asp.
17) U.S. Const., Art. I, Sec. 10.
18) Brian Carlson, 30 Common Logical Fallacies–A Study Starter, ACADEMIC INFLUENCE (Jul. 23, 2021), available at https://academicinfluence.com/inflection/study-guides/logical-fallacies.
19) What is Data Localization?, CLOUDFLARE (n.d.), available at https://www.cloudflare.com/learning/privacy/what-is-data-localization/.
20) Erol Yayboke, Caroline G. Ramos, & Lindsey R. Sheppard, The Real National Security Concerns over Data Localization, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (Jul. 23, 2021), available at https://www.csis.org/analysis/real-national-security-concerns-over-data-localization.
21) EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield, EUROPEAN COMMISSION (Feb. 2, 2016), available at https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216.
22) E. L., The New Trnsatlantic Data "Privacy Shield", THE ECONOMIST (Feb. 2, 2016), available at https://www.economist.com/the-economist-explains/2016/02/02/the-new-transatlantic-data-privacy-shield.
23) Commissioner Jourová's Remarks on Safe Harbour EU Court of Justice Judgement before the Committee on Civil Liberties, Justice and Home Affairs (Libe), EUROPEAN COMMISSION (Oct. 26, 2015), available at https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_15_5916.
24) Article 29 working party archives 1997 – 2016, EUROPEAN COMMISSION (2016), available at https://ec.europa.eu/justice/article-29/documentation/index_en.htm.
25) Privacy Shield: More Robust and Sustainable Solution Needed, EUROPEAN DATA PROTECTION SUPERVISOR (May 30, 2016), available at https://web.archive.org/web/20160625142411/https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf.
26) European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows, EUROPEAN COMMISSION (Jul. 12, 2016), available at https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461.
27) Donald J. Trump, Executive Order: Enhancing Public Safety in the Interior of the United States, THE WHITE HOURS (Jan. 25, 2017), available at https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/.
28) Joseph R. Biden, Executive Order on the Revision of Civil Immigration Enforcement Policies and Priorities, THE WHITE HOURS (Jan. 20, 2021), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-the-revision-of-civil-immigration-enforcement-policies-and-priorities/.
29) Pub. L. 114-126, JUDICIAL REDRESS ACT OF 2015 (2015), available at https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf.
30) Phil Muncaster, Trump Order Sparks Privacy Shield Fears, INFO SECURITY (Jan. 27, 2017), available at https://www.infosecurity-magazine.com/news/trump-order-sparks-privacy-shield/
31) EU-US Privacy Shield for Data Struck Down by Court, BBC NEWS (Jul. 16, 2020), available at https://www.bbc.com/news/technology-53418898.
32) David McCabe, & Martina Stevis Grindal, U.S. and European Leaders Reach Deal on Trans-Atlantic Data Privacy, THE NEW YORK TIMES (Mar. 25, 2022), available at https://www.nytimes.com/2022/03/25/business/us-europe-data-privacy.html.
33) Standard Contractual Clauses (SCC), EUROPEAN COMMISSION (Jun. 4, 2021), available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
34) The Organisation for Economic Co-operation and Development (OECD) has codified the Fair Information Privacy Practices (FIPPs) guidelines into the following eight principles: (1)Collection Limitation Principle; (2) Data Quality Principle; (3) Purpose Specification Principle; (4) Use Limitation Principle; (5) Security Safeguards Principle; (6) Openness Principle; (7) Individual Participation Principle; and (8) Accountability Principle
35) Tech Target Staff, Fair Information Practices (FIP), TECH TARGET (Mar, 2011), available at https://www.techtarget.com/whatis/definition/Fair-Information-Practices-FIP.

36) OECD Staff, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (n.d.), available at https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
37) Garry Kranz, Gramm-Leach-Bliley Act (GLBA), TECH TARGET (Jun. 2021), available at https://www.techtarget.com/searchcio/definition/Gramm-Leach-Bliley-Act.
38) Peter F. Edemekong, Pavan Annamaraju, & Micelle J. Haydel, Health Insurance Portability and Accountability Act, NATIONAL LIBRARY OF MEDICINE (n.d.), available at https://www.ncbi.nlm.nih.gov/books/NBK500019/.
39) HHS Staff, HITECH Act Enforcement Interim Final Rule, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (Jun. 16, 20917), available at https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.
40) DOE Staff, Family Educational Rights and Privacy Act (FERPA), U.S. DEPARTMENT OF EDUCATION (Aug. 25, 2021), available at https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
41) FTC Staff, CAN-SPAM Act: A Compliance Guide for Business, Federal Trade Commission (Jan. 2022), available at https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business.
42) United States v. Katz, 389 U.S. 347, 388 (1967).
43) Understanding Data Privacy: A Compliance Strategy Can Mitigate Cyber Threats, THOMPSON REUTERS (n.d.), available at https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-a-compliance-strategy-can-mitigate-cyber-threats.
44) John P. Mello, 5 Keys to Data Protection Compliance, TECHBEACON (n.d.), available at https://techbeacon.com/security/go-beyond-policy-5-keys-data-protection-compliance.
45) Jay Rosen, How to Reposition Compliance as a Revenue Generator, CORPORATE COMPLIANCE INSIGHTS (Apr. 18, 2019), available at https://www.corporatecomplianceinsights.com/how-to-reposition-compliance-as-a-revenue-generator/.
46) Drayton Mayers, Strong Cybersecurity Can Be a Revenue Generator – Here Is Why and How, MEMPHIS BUSINESS JOURNAL (May 20, 2020), available at https://www.bizjournals.com/memphis/news/2020/05/20/strong-cybersecurity-can-be-a-revenue-generator.html.
47) PAUL KRUGMAN, & ROBIN WELLS, ECONOMICS (Worth Publishers 6th ed. 2021).