Volume 1, Number 1 January–February 2024

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL

fastcase FULL COURT PRESS

The Global Regulatory Developments Journal

Volume 1, No. 1 January–February 2024

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL (ISSN 2995-7486) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint.

For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

The photo on this journal's cover is by Gaël Gaborel—A Picture of the Earth on a Wall—on Unsplash

Cite this publication as:

The Global Regulatory Developments Journal (Fastcase)

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to international attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and others interested in global regulatory developments.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at morgan.wright@vlex.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2995-7486

Editor's Note

Welcome!

Victoria Prussen Spears*

Welcome to the inaugural issue of *The Global Regulatory Developments Journal*!

Several months ago, vLex and Fastcase, two of the largest and fastest-growing legal technology companies, merged to form the world's largest law firm subscriber base with more than one billion legal documents from more than 100 countries.

Shortly after, they approached my partner, Steven Meyerowitz, and me to discuss developing a global regulatory developments journal, reflecting the growing need for high-level, authoritative global regulatory developments information—and reflecting the global content and reach of vLex and Fastcase.

Now, we are very excited to launch *The Global Regulatory Developments Journal*, adding to the three preeminent journals we currently edit for Fastcase and vLex: *The Journal of Robotics, Artificial Intelligence & Law*, *The Journal of Federal Agency Action*, and *The Global Trade Law Journal*.

Our Mission

The Global Regulatory Developments Journal, which publishes six times per year, covers topics of interest to international attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and anyone interested in global regulatory developments.

The Global Regulatory Developments Journal is a subscription journal that examines developments on the hottest topics in international regulation today, particularly focusing on these five international areas of great significance:

1. Privacy and Cybersecurity;
2. Global Finance and Investments;
3. Climate and Energy;

The Global Regulatory Developments Journal / January–February 2024, Vol. 1, No. 1, pp. 5–7.

ISSN 2995-7486.

4. Technology; and
5. International Labor and Employment.

In This Issue

In this issue, we have articles on a wide range of global regulatory subjects from a similarly broad range of authors, including on:

- The challenges of foreign security futures, from Katten Muchin Rosenman LLP;
- Employer considerations for international remote work requests, from Fisher Phillips;
- LIBOR, from Baker & McKenzie LLP;
- Regulatory challenges complicating development of international green hydrogen projects, from King & Spalding LLP;
- The EU Data Governance Act, from Alston & Bird LLP;
- The UK's Extension to the EU-U.S. Data Privacy Framework, from Morrison & Foerster LLP;
- China's new draft rules regarding data export, from Wilmer Cutler Pickering Hale and Dorr LLP;
- India's new data privacy law, from Morrison & Foerster LLP; and
- Autonomous vehicle regulation in the United Arab Emirates, from Bracewell LLP.

Our Board

We also are especially proud of the leading global regulatory lawyers who have agreed to join our Board of Editors. In alphabetical order, they are

- Tyler Bridegan, Wiley Rein LLP;
- Paulo Fernando Campana Filho, Campana Pacca;
- Hei Zuqing, International Business School, Zhejiang University;
- Justin Herring, Mayer Brown LLP;
- Lisa Peets, Covington & Burling LLP; and
- William D. Wright, Fisher Phillips.

Contact Us!

We would like to hear from you. You can reach Steven Meyerowitz, the Editor-in-Chief, at smeyerowitz@meyerowitzcommunications.com, and you can reach me at vpspears@meyerowitzcommunications.com.

Enjoy the issue!

Note

* Victoria Prussen Spears, Editor of *The Global Regulatory Developments Journal*, is a writer, editor, and law firm marketing consultant for Meyerowitz Communications Inc. A graduate of Sarah Lawrence College and Brooklyn Law School, Ms. Spears was an attorney at a leading New York City law firm before joining Meyerowitz Communications. Ms. Spears, who also is Editor of *The Journal of Robotics, Artificial Intelligence & Law*, *The Journal of Federal Agency Action*, and *The Global Trade Law Journal*, can be reached at vpspears@meyerowitzcommunications.com.

The Manifold Compliance Challenges of Foreign Security Futures

Stephen R. Morris and Eli Krasnow*

In this article, the authors discuss the challenges facing in-house lawyers and compliance officers tasked with creating and monitoring compliance with the procedures and processes designed to achieve compliance with the Securities and Exchange Commission's 2009 exemptive order on foreign security futures.

Aristotle cites the "tragelaph" (the mythical "goat-stag") as an example of how a concept can have meaning without existing.[1] A "security future" is the U.S. financial system's "goat-stag": a concept packed with meaning but non-existent on the securities and futures exchanges of the nation. By contrast, foreign security futures congregate in thick herds in the listings of non-U.S. exchanges (where, it should be said, they are categorized simply as listed derivatives rather than as the part-security/part-futures hybrid that is unique to U.S. regulation).

By now, more than 14 years after the fact, the industry is familiar with many of the manifold compliance challenges the 2009 exemptive order on foreign security futures from the Securities and Exchange Commission (SEC) presents to broker-dealer/futures commission merchants (FCMs) that facilitate transactions in those products (as well as to their customers looking to trade them).[2] It was the growing awareness of those challenges that moved FIA Tech to develop the FSF Databank[3] tool that provides a month-end snapshot of each security and security index underlying the broad-based security index futures and foreign security futures contracts listed on non-U.S. exchanges globally and analyzes its status as broad- or narrow-based (for the indices) and whether it passes the primary trading market test under the 2009 Order (for all single-name and narrow-based security index futures).[4]

The FSF Databank is a critical tool for broker-dealer/FCMs looking to implement procedures and processes reasonably designed to achieve compliance with the 2009 Order. But by itself, it is not sufficient; the 2009 Order presents other challenges as well.

The Global Regulatory Developments Journal / January–February 2024, Vol. 1, No. 1, pp. 9–15.

ISSN 2995-7486.

Below is a catalog of those challenges intended to assist broker-dealer/FCM in-house lawyers and compliance officers tasked with creating and monitoring compliance with such procedures and processes.

The 2009 Order

But first, a quick synopsis of the main points of the 2009 Order. The 2009 Order defines two sets of compliance conditions governing transactions in foreign security futures involving a registered broker-dealer. (For its part, the Commodity Futures Trading Commission (CFTC) simply requires that customers for which FCMs facilitate transactions in foreign security futures be eligible contract participants (ECPs).)

Customer Conditions

The 2009 Order permits the following customers to transact in foreign security futures that satisfy the product conditions:

1. Qualified institutional buyers as defined in Rule 144A of the Securities Act of 1933 (Securities Act);
2. Non-U.S. persons as defined under Reg S under the Securities Act;
3. Registered broker-dealers effecting transactions on behalf of qualified institutional buyers (QIBs) or Reg S non-U.S. persons; and
4. Banks effecting transactions on behalf of QIBs or Reg S non-U.S. persons.

Product Conditions

The 2009 Order permits eligible customers to transact in foreign security futures that satisfy the following criteria:

- For futures on single securities, the security is issued by a foreign private issuer[5] and has its "Primary Trading Market" outside the United States, or the security is a debt

security issued by a foreign government that is eligible to be registered under Schedule B of the Securities Act.
- For futures on narrow-based security indices, at least 90 percent of the securities in the index, by number and by weight, are foreign private issuers and satisfy the Primary Trading Market test or debt securities issued by a foreign government that is eligible to register under Schedule B (and any issuers in the index that do not meet these criteria are subject to reporting under Section 13 or 15(d) of the Securities Exchange Act of 1934 (Exchange Act)).
- The futures contract is listed on an exchange not required to register under Section 5 of the Exchange Act and must clear and settle on a clearinghouse outside the United States (and the contract must not be closed or liquidated by transactions effected on a U.S. exchange registered under Section 6 or 15A of the Exchange Act).

A security is deemed to have its Primary Trading Market outside the United States if:

- At least 55 percent of the worldwide trading volume in the security took place in, on, or through the facilities of a securities market or markets located either (1) in a single foreign jurisdiction, or (2) in no more than two foreign jurisdictions during the issuer's most recently completed fiscal year.
- The trading in the foreign private issuer's security is in two foreign jurisdictions, the trading for the issuer's security in at least one of the two foreign jurisdictions must be greater than the trading in the United States for the same class of the issuer's securities in order for such security's primary trading market to be considered outside the United States.

Critically, under the Primary Trading Market test, American Depositary Receipts count.

Compliance Challenges

This article now turns to the catalog of compliance challenges that the FSF Databank is not currently designed to solve.

Contracts in Transition

The FSF Databank will tell you when a security index is "on the bubble" between broad-based and narrow-based but does not count trading days for contracts in transition between the two classifications to track the 45-trading-day test set forth under CFTC Rule 41.14. Currently, only exchanges track that day-by-day data. Market participants need to monitor communication from exchanges to track developments regarding contracts in transition.

Which Securities Act Exemption?

The 2009 Order frames transactions in foreign security futures as transactions in securities not involving a public offering. This means that the transactions must be made in reliance on an exemption from registration. So, which one? Although there's some language in the 2009 Order suggesting that market participants should consider Reg S as the best available exemption, the Order is nonetheless clear that broker-dealers must determine for themselves which exemption to rely on.

At least one non-U.S. clearinghouse has considered this issue and elected to rely on Reg D rather than Reg S, evidently out of concern that the SEC might view it to be involved in directed selling efforts in the United States. (Note that where clearing members facilitating transactions in foreign security futures for customers within the jurisdiction of the United States in reliance on Reg D must assure themselves that any such transaction with for a customer that is an accredited investor within the meaning of Reg D.)

Where does this leave broker-dealer/FCMs who need to determine which Securities Act exemption to rely on? The best answer appears to be: it depends on the circumstances. Reg D for exchanges involved in directed selling efforts into the United States; Reg S for exchanges that are not. In practical terms, this means diligence confirming that customers trading and clearing foreign security futures are (1) QIB/non-U.S. persons, and/or (2) accredited investors (as well as ECPs). It means documentation confirming the customer's agreement that foreign security futures transactions are offered and sold in private transactions not registered under the Securities Act; may not be publicly distributed, re-offered, resold, or otherwise transferred in the United States; and are entered into on an unsolicited basis (i.e., by the broker-dealer/FCM).

Foreign Private Issuers

Issuers of securities that are the underlying of foreign single-name security futures and (90 percent of the components of) narrow-based indices that are the underlying of foreign narrow-based security index futures must be foreign private issuers. There are two tests to determine whether a foreign company qualifies as a foreign private issuer: the first relates to the relative degree of its U.S. share ownership, and the second relates to the level of its U.S. business contacts. A foreign company will qualify as a foreign private issuer if 50 percent or less of its outstanding voting securities are held by U.S. residents; or if more than 50 percent of its outstanding voting securities are held by U.S. residents and none of the following three circumstances applies: the majority of its executive officers or directors are U.S. citizens or residents, more than 50 percent of the issuer's assets are located in the United States, or the issuer's business is administered principally in the United States.

Most broker-dealer/FCMs will have access to databases that can be mined to extract this information about any non-U.S. issuer, but, as should be evident from the complexity of the test, it is not a straightforward exercise.

Schedule B Issuer Status

Futures on securities issued by foreign governments or political subdivisions thereof (other than the 21 governments listed in Security Exchange Act Rule 3a12-8)[6] are eligible under the product conditions set forth in the 2009 Order only if the foreign government issuer is eligible to be registered as a Schedule B issuer. Again, most broker-dealer/FCMs will have the means to determine whether a foreign government is an eligible Schedule B issuer (but may not be readily accessible to personnel covering the trading desks that handle foreign security futures).

Issuers in Narrow-Based Indices That Do Not Satisfy the Primary Trading Market Test

A narrow-based security index that passes the primary trading market test may include a handful (no more than 10 percent, by volume and weight in the index) of names that do not satisfy that

test. For such an index to remain eligible under the Product Conditions in the 2009 Order, those names must be subject to reporting under Section 13 or 15(d) of the Exchange Act. In essence, this requirement says that if an issuer does not pass the primary trading market test (that is, its securities are "primarily" traded on U.S. registered markets), then it should be subject to Exchange Act reporting (annual, quarterly, and other current reports, including 8-K and 13F filings). Once again, this is information broker-dealers will have, but trading desk coverage will need to track it down.

Exchange and Clearinghouse Eligibility

Eligible foreign security futures must be listed on a non-U.S. not required to register under Section 5 of the Exchange Act and must clear and settle on a clearinghouse outside the United States (and the contract must not able to be closed or liquidated by transactions effected on a U.S. exchange registered under Section 6 or 15A of the Exchange Act).

The diligence around these compliance conditions involves a combination of confirming that an exchange is, in fact, not a national securities exchange registered with the SEC, that the broker-dealer/FCM is not offering "direct access" to transactions in foreign security futures listed on the non-U.S. exchange in question (which could trigger the requirement to register and would likely breach the exchange's terms of access), the clearinghouse is not located in the United States, and that transactions in the relevant contract cannot be executed through the facilities of a registered exchange (even if the mode of execution under consideration does not leverage such facilities).

Notes

* The authors, attorneys with Katten Muchin Rosenman LLP, may be contacted at stephen.morris@katten.com and eli.krasnow@katten.com, respectively.

1. Aristotle, De Interpretatione, Section 1.1.

2. The SEC's 2009 Order is available at https://www.sec.gov/files/rules/exorders/2009/34-60194.pdf.

3. More information about the FSF Databank is available at https://fia-tech.com/products/databank/.

4. The authors' firm has partnered with FIA Tech to provide commentary about regulatory developments affecting the quantitative analysis presented by the FSF Databank.

5. Additional information about the foreign private issuer test is available at https://www.sec.gov/divisions/corpfin/internatl/foreign-private-issuers-overview.shtml#IIA.

6. *See* 17 CFR § 240.3a12-8—Exemption for designated foreign government securities for purposes of futures trading.

Employer Considerations for International Remote Work Requests

Nazanin Afshar*

In this article, the author explains what employers should consider when employees request cross-border remote status.

As we emerge from the prolonged COVID-19 pandemic, many employers are grappling with questions regarding whether and to what extent they should require employees to return to the office. Many employees want to continue working remotely at an international location—either on a long-term or permanent basis. An increasing number of employers are considering and granting these requests and transitioning their employees toward cross-border remote status. But is it the right choice for your organization?

Employers' Considerations

When considering whether to grant an employee's request to work remotely, employers must understand the breadth and scope of what they are being asked to do, what their options are, and the pros and cons of those options. From a high-level perspective, some questions employers must consider include:

- Which jurisdiction's employment law applies?
- How are the pay or payroll-related logistics going to be structured and managed?
- Are there any immigration issues that need to be addressed by the company?
- How can we ensure the organization is complying with applicable tax laws?
  - What income taxes are owed?
  - Are we purposely or inadvertently creating a "Permanent Establishment"?

The Global Regulatory Developments Journal / January–February 2024, Vol. 1, No. 1, pp. 17–24.

ISSN 2995-7486.

- What expenses, if any, need to be reimbursed and should that be structured?
- What benefits and insurance will we provide and how will those be administered?
- Are there any applicable health and safety rules we need to enforce or abide by?
- Are there any government agencies with which we need to register?
- What are works councils, and does the company need to establish one?
- How do we manage the employees' performance and which, if any, monitoring tools may we use?
- What is the social and political climate in the location where the employee wishes to work?

As a company's global footprint expands, the complexity only increases.

Indeed, since the COVID-19 pandemic, countries around the world have been enacting new legislation or adopting new frameworks governing remote work, hybrid or flexible work schedules, telework or telecommuting, and other similar concepts to keep up with these trends and stay competitive in the global economy. For example, some countries have made it easier for foreigners to stay and work remotely, such as the Extended Stay Visa in the Bahamas and the Remote Workers' Visa in Costa Rica. Other countries[1] have enacted new legislation that governs a variety of topics in this space, including how remote work agreements are to be memorialized, what terms those agreements need to include, how certain employees need to be paid, whether employees are entitled to "disconnect," which governmental and quasi-governmental entities need to be notified of these agreements, what expenses must or can be reimbursed, and so forth.

So, with such a complex web of issues to navigate, why should an organization permit remote work at all?

What Are the Benefits of Permitting Some Form of Remote Work?

From a risk and compliance perspective, permitting employees to work remotely, especially internationally, can seem like more

trouble than it is worth. However, variations on the traditional concept of the workplace are the new normal, and some market research suggests that employees prefer and even demand some flexibility to work remotely at least part of the time. At least one study showed that companies requiring their employees to return to work were more likely to lose top talent and suffer higher rates of attrition.[2]

There may be practical benefits to permitting some form of remote work as well. For example, remote work can potentially increase workforce participation (including those who might not otherwise be able to work due to family or other constraints), increase productivity, flexibility, and employee satisfaction, and reduce commuting time and exposure to related perils, such as traffic accidents and pollution.

What Are the Different Types of Remote Work and What Do They Mean?

Telework or telecommuting. Remote work. Flexible work arrangements. The definitions of these terms, as well as whether they can be used interchangeably, vary from jurisdiction to jurisdiction. In general, the following definitions apply:

- A flexible work arrangement is a more general term whereby a company can agree to relax rules or otherwise provide flexibility in the workplace to employees. It is not only limited to the place of work and can include, by way of example, casual dress days, flexible scheduling of workdays, work shift start/end times, or other parameters, or optional telecommuting on an ad hoc or set schedule basis.
- Telecommuting is a type of flexible working arrangement whereby the company agrees that individuals may work outside of a company's traditional office or workspace, and instead work at their home or other location. These employees use technology to conduct work and to communicate with their managers and co-workers. This can also be referred to as "remote work" and, if done at home, could also be referred to as "work from home" or "WFH."
- Hybrid work is another type of flexible working arrangement where employees work one part of their schedule

> (i.e., one or more days per week) in the company's physical workspace and the other part remotely, either at their home or another location. The employer and employee can agree in advance which days will be in office versus at home, or the employer can permit the employee the freedom to choose.

Although there is some overlap in these definitions, there are instances where it is important to be specific and clear on what the arrangement is so that all involved can determine what rules apply. For example, a January 2021 reform to the Federal Labor Law in Mexico applied to workers who perform paid work at least 40 percent of the time outside the workplace. New remote working legislation in Spain, also enacted in 2021, applied to "regular" remote workers, defined as those who perform at least 30 percent of their total hours remotely over any three-month period. In Colombia, "telework," "work from home," and "remote work" are distinct terms that are regulated by different laws.

Restrictions

In the traditional workplace, monitoring and managing employee performance is not without its difficulties in terms of interpersonal relationships, workplace morale, and other factors. In the context of remote or other non-traditional work relationships, there are other issues to consider—some of which only became apparent in recent years.

One example of this is workplace monitoring, including keeping track of employees' calls or messages, activity-tracking software, and audio or video monitoring or recording. As remote work has become more prevalent, so has the use of technology as a tool for employers to observe their employees' productivity. In some jurisdictions, such technologies if used improperly can run afoul of existing laws, such as the European Convention for the Protection of Human Rights and Fundamental Freedoms. And employers can run risks if they try to apply a one-size-fits-all approach to all employees regardless of where those employees are located, or if those policies go beyond employees' reasonable expectations. For example, in early 2023, a Dutch court ordered an American company to pay approximately €75,000 after the company terminated

the employee, a Dutch citizen, for refusing to keep his camera on all day in violation of his fundamental right to a private life.[3]

Another issue is the employee's right to disconnect, which refers to legislation that allows workers to establish a boundary between work and home life and not receive or answer any work-related emails, calls, or messages outside of normal working hours. France was the first European country to introduce legislation on this topic back in 2017. Since then, several other countries in Europe (including Belgium, Ireland, Italy, and Portugal) and in the Western hemisphere (including Argentina, Chile, Ecuador, and Mexico) have enacted similar laws and policies.

Logistics

An employer's obligation to reimburse remote workers' expenses not only depends on the laws of the country or state in which you are located but also may depend on the country or state that the remote employee is living and working in. This is especially true if the country or state is different than your location. Generally, the laws of the country or state where the employee performs services will apply to the employment relationship. The longer the employee works from another country or state, the more likely the local law will apply.

As with other topics mentioned in this article, knowing the location of the employees is incredibly important because the laws can vary greatly.

For example, some countries, such as Australia, Canada, India, and the United Kingdom, impose no legal obligation on employers to reimburse employees for expenses that the employees incur while working remotely.

By contrast, many other countries, such as Brazil, China, Italy, and Spain, impose a general requirement that employers must reimburse employees for any business expenses, which include equipment employees need in order to work remotely, such as computers and desks. There are a few countries, such as Colombia, the Czech Republic, France, and Mexico, that require employers to reimburse employees for all remote work expenses, including a proportionate share of the employees' utilities costs.

Or consider Japan, New Zealand, or South Africa, where there is no explicit statute requiring employers to reimburse employees

for remote work expenses, but reimbursements are highly recommended to avoid claims of discrimination or claims based on negative changes in working conditions.

Conclusion

As the world of COVID-19 changed all of our lives, the world of work continues to evolve, and it is evolving at a pace far quicker than laws around the world can keep up with. Employers would do well to understand that while technology, philosophy, convenience, and economics all point to the changing work environment that allows employees to "work from anywhere," care must still be taken to ensure legal compliance. The concerns laid out above should not be an afterthought. Before permitting employees to work remotely at an international location—either on a long-term or permanent basis—a careful review of compliance obligations should be undertaken.

What Can Employers Do to Be Ready When Remote Work Requests Come In? An 11-Step Response Strategy

1. *Be ready*. Have a checklist of questions to ask in the event an employee makes such a request.
2. *Budget sufficient time*. Do not rush into any decisions and be sure to give yourself and/or company management adequate time to review the issues, to work with stakeholders and counsel on a plan of action, and to implement any necessary steps prior to granting the employee's request.
3. *Information finding*. Take time to understand the organization's legal obligations in the different states, countries, or other areas where the employee works or requests to work. It is incredibly important to identify the locations so you can identify the specific laws in each of those places as it pertains to employment, immigration, taxes, data privacy, and all of the other considerations noted in this article.

4. *Determine the company's financial commitment and risk appetite*. Familiarize yourself or your organization's leadership with these concepts and discuss what the organization is willing to do in general.
5. *Negotiate terms with the employee*. Work with the employee to understand what they are looking for and document communications to keep a record of what has been discussed, including what concepts or terms have been considered and rejected.
6. *Formalize agreements*. In virtually all jurisdictions outside the United States, an employment arrangement must or should be memorialized in an agreement signed by the employee and an authorized agent of the employer. Make sure these agreements contain all necessary terms, especially including any terms pertaining to flexible work arrangements, performance metrics or expectations, compensation and benefits, and so forth.
7. *Establish support structure (e.g., incorporation, local service providers, etc.)*. Get to know the jurisdiction you will be operating in and what you will need to have employees there, including whether your company needs to register or incorporate locally, whether you should engage a local employer of record, local payroll company or tax advisor, and any other support systems. Work with counsel to ensure you have not missed anything.
8. *Have policies in place*. Your home country handbook is probably not sufficient to cover all contingencies, especially if you are expanding your operations overseas. If you need policy documents, internal work regulations, or similar documents to establish and maintain control over your organization's operations in other locations, work with your counsel to determine what you need and how best to implement it.
9. *Report to government agencies where required*. In some locations, the employer is required to pay for social insurance on its employees' behalf. In other locations, the employer must register with the local

workers' compensation and workplace safety agencies. Be sure to identify and comply with all such requirements, particularly where non-compliance can result in fines or penalties, public censure, or other negative consequences.

10. *Periodic compliance check and audit*. Employee handbooks should be reviewed and/or updated every year to ensure compliance with legislative and other changes. The same concept applies to your organization's global operations and the parameters thereof.
11. *Set reminders to review the arrangement on key dates*. Incorporate a reservation of rights into your policies or employment agreements that will enable you to review your situation and make changes as needed.

Notes

* Nazanin Afshar, a California-based attorney at Fisher Phillips and a member of the firm's International Employment Practice Group, has counseled clients transitioning employees to remote work in over 40 jurisdictions, drafted employment agreements for U.S.-based companies with employees working outside the United States, and provided guidance on employment decisions such as investigations and terminations. The author may be contacted at nafshar@fisherphillips.com.

1. The growing list of jurisdictions with new remote working legislation since 2019 includes Angola, Argentina, Belgium, Brazil, Chile, Colombia, Denmark, Greece, Italy, Luxembourg, Mauritius, Mexico, Norway, Peru, Philippines, Portugal, Russia, Slovakia, Spain, Sweden, Taiwan, Turkey, and Ukraine.

2. "Returning for Good" Report by Unispace, 2023.

3. Nazanin Afshar & Sophia Ellis, "U.S. Company's Mandatory Video Surveillance Violated Dutch Remote Workers' Fundamental Right to a Private Life," Feb. 10, 2023.

LIBOR Is Dead. Long Live *Synthetic* LIBOR!

Nick O'Grady, Mark Tibberts, Matthew Smith, John Lawlor, Gabby White, and James McErlean*

In this article, the authors explain that synthetic LIBOR offers a temporary reprieve for unremediated legacy contracts—but not without risk.

On Friday, June 30, 2023, the last rates based on the London Interbank Offered Rates (LIBORs) were published. This momentous day was the culmination of a long journey for the financial markets, as market participants moved into the future with alternative risk-free rates. However, work remains, in some jurisdictions more than others, to address legacy transactions and to understand what rate a U.S. dollar (USD) LIBOR contract may switch to following this date.

Further efforts will also be needed to transition away from interbank offered rates (IBORs) in some non-LIBOR currencies and to comply with the latest regulatory guidance on the use of robust contractual fallbacks to avoid the need for a rerun of the LIBOR transition process.

This article examines the current state of play and what actions financial institutions, asset managers, insurers, and corporates should take.

Key Takeaways

- As of July 1, 2023, LIBORs, as a measure of the interest rates on which key banks are willing to lend money in the short-term interbank market, no longer were published.
- Synthetic versions of one-, three-, and six-month USD LIBORs will be available until September 30, 2024. These will be published by ICE Benchmark Administration Limited in the same place and at the same times as the original USD LIBORs but will be constituted from different data, that is, CME Group's Term Secured Overnight Financing Rate (SOFR) rates together with fixed credit spread adjustments.

The Global Regulatory Developments Journal / January–February 2024, Vol. 1, No. 1, pp. 25–34.

ISSN 2995-7486.

- A number of mechanisms can provide a temporary reprieve or technical solution for unremediated contracts; namely synthetic USD LIBOR, the U.S. Adjustable Interest Rate (LIBOR) Act (US LIBOR Act), and the ISDA IBOR Fallbacks Protocol. Nonetheless, all market participants with unremediated legacy contracts should do the following:
  - Assess what interest rates will apply to those contracts after 30 June 2023 (e.g., a contractual fallback rate, a statutorily imposed replacement rate or synthetic LIBOR); and
  - Actively continue to progress amendments to the interest rate terms of legacy contracts wherever possible.
- For USD loans, Term SOFR (as opposed to Compounded in Arrears SOFR or Daily Simple SOFR) is proving the most popular replacement rate. Some regulators, and the Financial Stability Board, are apprehensive about the widespread use of Term SOFR and would prefer more transactions to be overnight SOFR-based wherever achievable. We expect them to continue to monitor the adoption of Term SOFR and, if necessary, issue further guidance on its use.
- There are no current plans for EURIBOR (Euro Interbank Offered Rate) to cease, but European regulators have recently reiterated their guidance for parties to ensure that their EURIBOR-based contracts include robust fallbacks should EURIBOR become unavailable. Parties should consider including a rate switch mechanism in new euro loan contracts to effect an automatic conversion from EURIBOR to €STR (the euro risk-free rate) upon the cessation of EURIBOR or EURIBOR ceasing to be representative of lending costs.
- With forward-looking term rates based on €STR now available for use in transactions, these rates, which are operationally (if not economically) similar to EURIBOR, may encourage transition in euro-denominated products.
- Work on IBOR transition will continue for some time as other currencies progress toward the use of risk-free rates.

U.S. Dollars—Transition Progress

The day some never believed would come has finally arrived. Friday, June 30, 2023, marked the last publication date for any LIBOR—at least in its current form.

Over the past few years, the finance world has been weaning itself off the use of LIBORs as an interest rate basis for financial products. This seismic change has progressed at sometimes varying paces with pauses and punctuation marks along the way.

Perhaps the most significant moment came on March 5, 2021, when the UK's Financial Conduct Authority (FCA) set out the final timetable for LIBOR's demise.[1] At that time, it was recognized that, of the five LIBOR currencies, USD LIBORs were the most widely used and systemically important of those rates and more time should be given for an orderly transition for USD LIBORs than for the other LIBOR currencies (pound sterling, Swiss franc, Japanese yen, and euro).

While December 31, 2021, marked the end of all non-USD LIBORs (although in the case of certain pound sterling and Japanese yen tenors, synthetic versions remained available for a longer period), the one-, three-, and six-month tenors of USD LIBOR were allowed to continue until June 30, 2023. This has contributed to the slower pace of LIBOR transition for USD-denominated contracts than that of other LIBOR currencies. However, a combination of regulatory initiatives, legislation, industry working group efforts, education, the forming of market consensus, increasing liquidity in SOFR trading, and hard work from market participants have ensured that great strides have been made in recent months.

The areas of greatest concern revolve around legacy contracts that continue to reference USD LIBOR.

- In the United States, the most recent readout from the Alternative Reference Rates Committee's (ARRC) May 25, 2023, meeting[2] noted that "respondents [in the most recent sentiment survey of ARRC members] continued to characterize the LIBOR transition overall as progressing smoothly or generally smoothly in 2023." However, it is anticipated that a significant stock of USD LIBOR exposures will remain outstanding, which do not benefit from suitable fallback provisions.
- In Japan, the results of a survey on the use of LIBOR[3] undertaken by the Financial Services Agency and Bank of Japan at the end of December 2022 (and published on March 24, 2023) found that "almost 60 percent of financial institutions either have no existing contract or have completed an active transition [of contract referencing USD LIBOR]" and that "financial institutions with legacy

contracts responded that they did not have major obstacles to transition arrangements at this point."

- In the European Union, the minutes of a meeting of the Working Group on Euro Risk-Free Rates held on April 3, 2023[4] covered the results of a USD LIBOR survey of the members of the working group and noted "a material decline of the total number of tough legacy contracts and of the total exposures corresponding to such tough legacy contracts, both for derivatives and cash products," but that "[s]imilar to the previous survey [in July 2022], bilateral and syndicated loans are the asset class with the largest tough legacy exposure, followed by derivatives and bonds."
- The situation is less advanced in some other jurisdictions. The Financial Stability Board's (FSB) Progress Report on LIBOR and Other Benchmark Transition Issues[5] (published on December 16, 2022) noted strong progress in many jurisdictions and that the majority of post–June 30, 2023, USD LIBOR exposures would be in derivatives. However, the 24 non-FSB members surveyed (including Bahrain, Chile, Ghana, and Malaysia) estimated that around USD 0.483 trillion of U.S. dollar assets, USD 0.033 trillion of liabilities and USD 0.971 trillion of derivatives exposures would remain after June 30, 2023, and highlighted issues such as "most contracts are pending renegotiation," "uncertainty about the remaining proportion of exposures," and the identification of "several issues around system readiness." Further progress will have been made since that report but, nonetheless, more work remains.

LIBOR transition has, to some degree, been slowed by the general macroeconomic conditions. In particular, inflationary pressures that have led some central banks to increase interest rates over the past 12 months or so have reduced some natural opportunities for amending legacy contracts as corporates may have been reluctant to refinance into higher rates. Bank credit tightening may also have had an effect on amending legacy terms. These factors have also complicated the debate around appropriate credit spread adjustments, which are intended to ensure there is no (or minimal) transfer of economic value as a result of the transition; the ISDA fixed credit spread adjustments were set by reference to the mean difference between each tenor of USD LIBOR and SOFR

(compounded over the same period as the relevant tenor) over the five years preceding March 5, 2021. In the two-plus years since that calculation date, the spot spread has varied and informed debtor/creditor negotiations. An increase in distressed credits also complicates transition discussions.

U.S. Dollars—After June 30, 2023

For contracts that remain unremediated, what happens after June 30, 2023? It depends on the type of contract, any relevant contractual fallbacks, and such contract's governing law. Described below are the possibilities:

- *Contractual Fallback Language*: Some contracts have fallback language that will implement a switch to a new benchmark interest rate. For example, English law loan agreements may include a rate switch mechanism that automatically flips the interest rate basis from USD LIBOR to CME Term SOFR or Compounded in Arrears SOFR. Parties to a non-cleared derivative contract (e.g., an International Swaps and Derivatives Association (ISDA) Master Agreement) may have adhered to the ISDA IBOR Fallbacks Protocol that automatically effects a change from USD LIBOR to SOFR plus a fixed credit spread adjustment after June 30, 2023. However, some contracts have no contractual fallback. For these contracts, if the loan agreement is governed by the law of a U.S. state, the U.S. LIBOR Act may apply, as described below.
- *Synthetic USD LIBOR*: Synthetic USD LIBOR is another possibility. The FCA confirmed that it will exercise its powers to compel ICE Benchmark Administration Limited to publish one-, three-, and six-month tenors of "synthetic" USD LIBOR until September 30, 2024. The methodology for these synthetic rates will use the relevant CME Term SOFR rate plus the respective ISDA fixed credit spread adjustment.

  The UK Critical Benchmarks (References and Administrators' Liability) Act 2021 clarifies that a reference in a contract or other arrangement to LIBOR should, for all purposes, be treated as a reference to the relevant synthetic

LIBOR. This aims to ensure contractual continuity, although its efficacy for non-UK law contracts will be a matter for the relevant jurisdiction in question.

Although representations were made to the FCA to retain flexibility to further extend the end date for synthetic USD LIBOR, it declined to do so. However, it did leave some "wiggle room" and have guided that:

> our current assessment that end-September 2024 provides sufficient time for cessation to be orderly is based on the information available to us.... We consider the evidence base for our assessment to be robust. Therefore, unless unforeseen and material events were to occur which significantly change the information and circumstances on which our assessment was based, we expect ... to follow the timeline we have indicated.

- *Designated Replacement Rates*: For agreements governed by the law of New York or another U.S. state, the U.S. LIBOR Act may apply. The U.S. LIBOR Act empowered the board of governors of the Federal Reserve System to select a replacement rate for any U.S.. law–governed contract that uses USD LIBOR as a benchmark, if such contract: (1) contains only fallback provisions based on USD LIBOR (e.g., a historic LIBOR) or on a poll of quoted rates; (2) does not contain any fallback provisions; or (3) contains fallback provisions that do not specify a specific replacement rate or a determining person. The statutory replacement rates[6] selected for corporate loans are the relevant tenor of CME Term SOFR, which corresponds to the applicable USD LIBOR tenor plus the applicable ISDA fixed credit spread adjustment. It was intentional that the U.S. and UK solutions for legacy contracts produce the same result.

Market participants should note that USD LIBOR loans that will bear interest by reference to synthetic USD LIBOR or the U.S. LIBOR Act–designated replacement rates may result in an imperfect hedge after June 30, 2023. The standard fallback rates for USD LIBOR hedging contracts, as set out in the ISDA IBOR Fallbacks Protocol and the rules of central counterparty clearing houses are

based on Compounded in Arrears SOFR plus the applicable ISDA fixed credit spread adjustment. As noted above, loans that will bear interest by reference to synthetic USD LIBOR or the U.S. LIBOR Act–designated replacement rates will bear interest at CME Term SOFR plus the applicable ISDA fixed credit spread adjustment. Thus, for hedged loans, active transition in order to ensure that the relevant hedging and loan benchmarks are in alignment is preferable.

As legacy contracts naturally come to the end of their terms, the stock of legacy USD LIBOR exposures will continue to reduce. However, the push for active transition should continue so parties can ensure that a sustainable and clear replacement rate is in place.

In the United States, the ARRC limitations on Term SOFR hedging continue to be strict. As a general matter, counterparties may only enter into a Term SOFR swap in order to hedge an existing position in a Term SOFR cash product or to use Term SOFR in connection with a fallback from a legacy USD LIBOR exposure.

Vice Chair Michael S. Barr of the U.S. Financial Stability Oversight Council stated:

> A world in which Term SOFR is used across all or most cash products is not a plausible one. Such a world would not be consistent with sustaining a robust market for overnight SOFR derivatives, the foundation for Term SOFR rates. Therefore, the use of Term SOFR must remain limited in line with the recommendations of the FSOC and Financial Stability Board.[7]

Many parties have chosen to transition their loans to a Term SOFR basis. It is clear that regulators wish to keep Term SOFR use to a minimum to avoid the risk that overnight SOFR may become less robust as a result of increased Term SOFR trading.

The ARRC limitations had led to less liquidity in the Term SOFR hedging market, and increased expense compared to hedging overnight SOFR.

Euros

While there are no current plans for EURIBOR to cease publication or be declared unrepresentative of the market it measures, market participants should note a number of recent developments. EURIBOR is a daily reference rate based on the average rate at

which Eurozone banks lend to each other on an unsecured basis in the interbank market, based on quotes from a panel of banks. As such, EURIBOR is not a risk-free rate and potentially has the same issues as LIBOR.

First, two administrators—Refinitv and the European Money Markets Institute (EMMI)—are now publishing forward-looking term rates that are based on €STR (the euro short-term rate) in various tenors. EMMI's offering has been publishing live rates since November 14, 2022, and can be used in transactions, while Refinitiv's version is currently only available on a beta basis. It is hoped that the availability of these rates will encourage wider usage of €STR in the loan markets.

Second, the Working Group on Euro Risk-Free Rates (Euro RFR WG) has recently updated its terms of reference. Part of the updated remit of the Euro RFR WG is to "foster the use of €STR in a diverse range of financial products."

To date, the use of €STR, whether in its pure overnight form or as a forward-looking term rate, appears to be very limited, and the majority of euro loans that we see do not provide "hardwired" provisions dealing with any possible cessation or non-representativeness of EURIBOR. The Euro RFR WG originally issued recommendations in May 2021 detailing suitable potential fallbacks to be included in documentation to cater for this. However, the response from market participants to date has been underwhelming. In an attempt to drive change, the Euro RFR WG recently issued further guidance to reiterate these fallbacks and noted that "[c]ost of funds and replacement of screen rate language are not workable permanent fallbacks and do not provide scalable options in the case of a possible permanent discontinuation of EURIBOR" and that:

> whilst EURIBOR is not scheduled to be discontinued, this does not negate the need for market participants to include robust fallback language in their contracts. Robust fallbacks are a requirement of the EU Benchmarks Regulation (BMR)....

The experience of LIBOR transition has shown that the combination of clear cessation dates and robust regulatory/supervisory "guidance" has been the catalyst for accelerating change. If European regulators start to police compliance with the Euro RFR WG recommendations more strictly, many more euro loans should

start to include "rate-switch" mechanisms that provide for an automatic switch from EURIBOR to Compounded in Arrears €STR or a forward-looking term €STR (EMMI's Efterm® or Refinitiv's Refinitiv Term €STR).

A clear cessation date for EURIBOR would kick-start adoption of €STR for new loans. In the meantime, a number of push and pull factors may, nonetheless, encourage loan market participants to move away from EURIBOR. The ingredients that have contributed to making a success of LIBOR transition (e.g., IT systems updates, recommended market conventions, template documentation, and the availability of forward-looking term rates) can be equally applied to any EURIBOR transition. There are few barriers, other than the parties' desires, to switching to €STR-based lending. On the other hand, we see continued efforts to improve the robustness of EURIBOR, including reforms to reduce reliance on expert determination, which signal its continued relevance for loan markets.

Other Currencies

Many other countries remain committed to reform regarding replacement of the relevant IBOR for their currencies.

In South Africa, the Johannesburg Interbank Average Rate (JIBAR) is due to be retired, with the South African Rand Overnight Index Average (ZARONIA) identified as a successor near risk-free rate. ZARONIA has been published since November 2, 2022, and its performance is currently being observed by market participants. This observation period ended November 3, 2023, with the expectation that trading in ZARONIA-based derivative products can commence soon afterward. While the exact timing is as yet unclear, the South African Reserve Bank has stated that it would prefer a relatively short JIBAR transition period.

In Canada, a two-stage transition plan is underway to move from the Canadian Dollar Offered Rate (CDOR) to the Canadian Overnight Repo Rate Average. After June 30, 2023, the Bank of Canada's guidance is that no new CDOR derivatives or securities will be permitted. After June 28, 2024, publication of all remaining CDORs will cease.

In Poland, the Warsaw Interbank Offered Rate is due to be replaced by the Warsaw Interbank Bid Rate by the end of 2024.

Notes

* Nick O'Grady and Mark Tibberts are partners in Baker & McKenzie LLP. Matthew Smith is counsel to the firm. John Lawlor is an attorney at the firm. Gabby White is a knowledge lawyer at the firm. James McErlean is a trainee solicitor at the firm. The authors may be contacted at nick.ogrady@bakermckenzie.com, mark.tibberts@bakermckenzie.com, matthew.smith@bakermckenzie.com, john.lawlor@bakermckenzie.com, gabby.white@bakermckenzie.com, and james.mcerlean@bakermckenzie.com, respectively.

1. FCA announcement on future cessation and loss of representativeness of the LIBOR benchmarks, https://www.fca.org.uk/publication/documents/future-cessation-loss-representativeness-libor-benchmarks.pdf.

2. https://www.newyorkfed.org/medialibrary/Microsites/arrc/files/2023/ARRC-Readout-May-2023-Meeting.pdf.

3. https://www.boj.or.jp/en/finsys/libor/data/lib230324a.pdf.

4. https://www.esma.europa.eu/sites/default/files/2023-05/EUR_RFR_WG_03_04_2023_Meeting_Minutes.pdf.

5. https://www.fsb.org/wp-content/uploads/P161222.pdf.

6. https://www.govinfo.gov/content/pkg/FR-2023-01-26/pdf/2023-00213.pdf.

7. https://www.newyorkfed.org/medialibrary/Microsites/arrc/files/2023/summary-of-key-arrc-recommendations-final-012523#%3A~%3Atext%3DA%20world%20in%20which%20Term%2Cfoundation%20for%20Term%20SOFR%20rates.

European Union Regulatory Challenges Complicating Development of International Green Hydrogen Projects

Frederick Lazell, Dan Feldman, Axel J. Schilder, Salomé Cisnal de Ugarte, John Clay Taylor, James F. Bowe Jr., and Zoë Bromage*

In this article, the authors examine guidance issued recently by the European Commission regarding EU rules defining green hydrogen and derivative fuels.

The EU rules defining green hydrogen and derivative fuels (such as ammonia, e-methanol, and electric natural gas (e-NG)) became binding law in June 2023. Subsequently, in late July 2023, the European Commission (EC) issued guidance, intending to aid the application of these rules, in the form of a Q&A document.[1]

However, in several areas, the guidance failed to deliver the regulatory clarity that project developers had been clamoring for. The EC guidance leaves developers seeking to export renewable fuels of non-biological origin (RFNBO) to Europe facing significant challenges in structuring their projects to meet the RFNBO requirements. Two of the most significant such challenges are:

1. The prohibition on state aid for renewable power generation where electricity is transmitted from a renewable generation facility to the RFNBO facility under a power purchase agreement (PPA) through the grid. This restriction is very broad and applies to state support provided outside the European Union.
2. The requirement for PPAs to be directly between RFNBO producer and renewable power generator. This restricts the use of sleeved PPAs or any structure with a utility supplier as an intermediary power supplier, or other participant in the contractual structure, raising issues in electricity markets that have state-mandated power purchasers and suppliers.

The Global Regulatory Developments Journal / January–February 2024, Vol. 1, No. 1, pp. 35–41.

ISSN 2995-7486.

Unless these issues can be resolved, projects that had been intending to produce RFNBOs for the European Union may look elsewhere for their markets (e.g., Asia is developing attractive demand-side subsidy mechanisms to support imports of green and low-carbon fuels). These technical issues may be serious enough for some in the industry to consider challenges before the Court of Justice of the European Union. Although it should be acknowledged that strictly the deadline for bringing a direct claim against the EC has passed.

Restriction on State Aid for Renewable Power Generation

One of the eligibility requirements for grid-transmitted power to be used for RFNBO production is that the renewable power installation must not have received any state aid.[2] This is a broad principle that prohibits any form of subsidy or other financial support for the construction or operation of the renewable power plant (including tax credits, grants, and preferential tariffs, among other things), with only limited exceptions.

Several countries around the world have implemented support schemes for renewable power projects, in part, to stimulate a green hydrogen industry and specifically contemplating that hydrogen-based fuels produced with renewable power could be exported to Europe. This includes the United States under the Inflation Reduction Act (IRA) (which allows the "stacking" of credits for different parts of the value chain), Canada through the investment tax credits announced in its 2023 budget, and Egypt, among others.

Why Is State Aid for Renewable Power Restricted?

The restriction on state aid forms part of the "additionality" test under the Additionality Delegated Act. In a general sense, showing "additionality" is a counterfactual test; that is, but for the demand for renewable power from the RFNBO producer, the renewables project would not have been developed. However, there is no single definition of additionality.

The EC has defined the additionality test that applies to RFNBO production under Article 5 of the Additionality Delegated Act. This requires that the renewable generation installation must be no older than 36 months from the date the RFNBO plant commenced operation and that the renewables facility has not received state aid.

The EC's decision to include this restriction on state aid makes the EU's version of additionality more onerous than even the strictest requirements being considered in the United States. Moreover, this decision is not, some in the industry argue, explicable by reference to the framework under the Renewable Energy Directive (RED II) authorizing the EC to adopt the Delegated Acts and to define the additionality principle to apply to RFNBO production.

The EC's authority to adopt the Additionality Delegated Act derives from Article 27(3) of RED II. This empowers the EC to define the "other appropriate criteria" that need to be met for grid-transmitted power to be eligible for RFNBO production. The scope of these criteria is circumscribed by the text of Recital 90 of RED II, which introduces the concepts of temporal and geographical correlation, as well as the additionality principle. In relation to additionality, Recital 90 states as follows: "[T]here should be an element of additionality [of the renewable power supply], meaning that the fuel producer is adding to the renewable deployment or to the financing of renewable energy."

Some argue that the parameters of the additionality principle in Recital 90 are significantly less strict than the final additionality test adopted by the EC in the Additionality Delegated Act. As a result, there have been suggestions in the industry that the EC could have exceeded its delegated authority under RED II. However, it is not yet clear whether there is the appetite or ability to turn such suggestions into a formal claim before the Court of Justice of the European Union.

This would, though, appear to be the only route that currently exists to remove the restriction on state aid. Absent this, projects need to carefully structure their power supply solutions so as to navigate around this restriction. States yet to implement support schemes may consider structuring these to provide higher levels of support for green hydrogen directly rather than indirectly via subsidies for renewable electricity production.

Restriction on Back-to-Back or Sleeved PPAs

The second major challenge facing developers is the statement from the EC in its July 2023 guidance that a PPA must be entered directly between the renewables generator and the RFNBO producer (i.e., no intermediary power supplier can be a contracting party to the power supply arrangements).[3] This is seen by some in the industry as a significant about-face from the EC.

PPA Arrangements Via Intermediaries

Article 5 of the Additionality Delegated Act requires RFNBO producers to show that they "have concluded directly, or via intermediaries, one or more renewables power purchase agreements" for the quantity of power used for RFNBO production. The reference to "or via intermediaries" was added during the negotiation process of the Additionality Delegated Act and was widely understood to allow an intermediary power purchaser and supplier to participate in the contractual structure between renewables generation and RFNBO production. This could be done through a back-to-back PPA arrangement (a form of sleeved PPA).

This was understood to be distinct from a virtual PPA structure, where unbundled renewable energy certificates (RECs) or guarantees of origin (GOs) are supplied to "green" the power supply to an electricity user. This use of unbundled RECs or GOs was never considered to be a possible power supply solution; the temporal correlation requirements in particular would, in any case, make this practically impossible.

There are two main scenarios (which may occur together) in which the back-to-back PPA structure is being considered by developers globally:

1. *Electricity markets with state-mandated power purchasers and suppliers*. In these markets, electricity consumers are not permitted to contract directly with renewable power generators, since local laws oblige (1) generators to sell to the state-mandated offtaker, and/or (2) consumers to purchase power from the state-mandated supplier (these may be different entities). This is the structure of many markets globally, including in the Middle East, North

Africa, Canada, and Central Asia (all of which are anticipated to be key sources of European imports of RFNBOs).

2. *Optimizing economics of renewables components and the grid services from green hydrogen production*. Under this structure, the renewables components are developed as a conventional renewable power project with a creditworthy utility as buyer of the power. This allows sponsors to achieve better economics through higher debt-to-equity ratios on the renewable power components. This optimizes the financial and commercial structuring of green hydrogen projects, because the intermediary's credit-strength standing behind the PPA could be used to support non-recourse financing of the renewables elements of a project. This structure also allows for the aggregation of electrons generated by several renewables projects (i.e., with multiple upstream PPAs aggregated by the utility into one downstream PPA) that would drive up the load factor and drive down the per-unit cost of green hydrogen production.

The utility then on-sells the same power, together with all RECS/GOs, to the RFNBO producer under a back-to-back PPA arrangement (complying also with all other RFNBO rules). A significant advantage of this structure is that it makes it easier for the utility (which either is, or interfaces with, the relevant transmission system operator) to optimize the potential for electrolyzers to act as flexible load, thereby providing grid-services from green hydrogen production. For example, at times of peak electricity demand, excess renewable power can be sold to the grid and the demand from the electrolyzer facility can be reduced to divert more renewable power to the grid.[4]

The EC's Requirement for Direct PPAS Only

However, the EC in its guidance of July 2023 stated that the role of the "intermediaries" in PPA arrangements can only be as "facilitator of such contracts but not as a contracting party."[5] This would therefore prohibit both of the back-to-back PPA scenarios described above. The EC states that this limitation is a result of the definition of a "renewables power purchase agreement" under

RED II, which is defined as a contract "to purchase renewable electricity directly from an electricity producer." However, it is not clear what the role of such facilitators would be (although they cannot be parties to the contractual arrangements). Such facilitators are not common features of large-scale power procurement activities globally in our experience.

Supplementary requests for clarification on this issue are pending before the EC, essentially seeking a reversal of this guidance or some other narrowing of its application. However, even if such reversal can be obtained, the EC's guidance is non-binding and so the mere existence of the earlier guidance requiring direct PPAs would create legal risk for developers. The only binding resolution to such an issue would be a decision of the Court of Justice of the European Union.

The EC's apparently strict limitation of the scope of the Delegated Acts within the confines of the letter of RED II in relation to the sleeved PPA issue stands in notable counterpoint to the discretion it is seen by some to have exercised in restricting state aid to renewables as part of the EU's additionality test.

Commercial Impact of These Restrictions

These issues create further uncertainty and legal risk for project developers seeking to export RFNBOs to the European market.

Ultimately, the state aid restriction risks denying European offtakers and consumers access to RFNBOs from many projects that seek to use subsidized renewable power transmitted through the grid. Furthermore, the requirement for direct PPAs will make it impossible for projects in many countries that will be crucial in meetings Europe's future energy demands to export product to Europe as RFNBO, absent a change in the local electricity market laws.

Cumulatively and individually these limitations on RFNBO eligibility may be expected to make it even more expensive for European fuel suppliers to source RFNBO to meet European demand. Confronted with these issues, the first RFNBO projects may have to turn to other markets to sell their product. If that happens, Europe risks losing its lead as both a key destination market for green hydrogen and derivative fuels and (relatedly) as an exporter

of the electrolyzers and other technologies required to produce the hydrogen to meet that demand.

Notes

* The authors, attorneys with King & Spalding LLP, may be contacted at flazell@kslaw.com, dfeldman@kslaw.com, aschilder@kslaw.com, scisnaldeugarte@kslaw.com, jtaylor@kslaw.com, jbowe@kslaw.com, and zbromage@kslaw.com, respectively.

1. https://energy.ec.europa.eu/system/files/2023-07/2023_07_26_Document_Certification_questions.pdf.

2. This restriction will apply from January 1, 2028; or, for RFNBO facilities commencing operations before that date, from January 1, 2038, but will then apply even to pre-existing RFNBO producers. The restriction only applies to grid-transmitted power: i.e., it does not apply to directly connected renewable power supply. The restriction applies to production projects both in and outside of the European Union.

3. https://energy.ec.europa.eu/system/files/2023-07/2023_07_26_Document_Certification_questions.pdf. *See* Q.16.

4. This has been recognized recently by France in its proposed low-carbon production support scheme, which is understood to contain bonus provisions for this kind of flexible load activity by hydrogen producers.

5. 2023_07_26_Document_Certification_questions.pdf (europa.eu). *See* Q.16.

What You Should Know About the EU Data Governance Act

Alice Portnoy and Wim Nauwelaerts*

In this article, the authors provide an overview of the EU's new Data Governance Act and discuss how the new law may impact businesses on both sides of the pond.

Data has become an essential resource for any modern economy. There is, however, a common perception that most data is not used efficiently and only a small group of businesses is able to extract value from it. To address this issue, EU legislators have adopted the Data Governance Act (DGA), which is now applicable.

In February 2020, the European Commission (EC) released its European Strategy for Data, designed to explore new ways to handle and create value from data. The strategy lays the foundation for a single market for data within the European Union, where data can circulate freely for the benefit of all while respecting the EU's fundamental values and principles.

As part of this strategy, the EC has taken several legislative initiatives with a view to facilitating data sharing across sectors and EU Member States. In May 2022, the EC adopted the first new law in this context: the DGA, which became effective on September 24, 2023. The DGA introduces new definitions, concepts, and enforcement mechanisms for the re-use of data by both public and private organizations. The DGA also includes new rules intended to encourage the voluntary sharing of data by individuals and organizations and establishes a regulatory framework for organizations acting as data-sharing intermediaries. The DGA's ultimate goal is to foster a new type of data governance that enables all stakeholders to (re)use data for innovative purposes.

The DGA is complemented by the Data Act, another legislative initiative that is part of the European Strategy for Data. The Data Act aims to optimize the accessibility and use of data generated by connected devices in the European Union (such as smart watches) by clarifying who can use such data and create value from it.

The Global Regulatory Developments Journal / January–February 2024, Vol. 1, No. 1, pp. 43–50.

ISSN 2995-7486.

The DGA is intended to supplement and interact with other EU laws that regulate data use, such as the General Data Protection Regulation (GDPR) and the Digital Markets Act. Organizations subject to the DGA may also have to consider these other regulatory frameworks.

Focal Areas of the DGA

The main goal of the DGA is to boost the development of reliable data-sharing platforms within the European Union and across sectors. To that end, EU legislators have focused on four key topics:

1. Re-use of data held by public sector bodies (PSBs) such as state, regional, or local authorities or other bodies and associations governed by EU public law.
2. Data intermediation services (DIS) that facilitate data sharing.
3. A new "data altruism" framework that encourages individuals and organizations to voluntarily share their data for the common good.
4. Rules to protect non-personal data against unlawful access by foreign authorities.

Re-Use of Data Held by Public Sector Bodies

In 2019, the EC adopted the Open Data Directive to regulate the re-use of publicly available information held by the public sector in each EU Member State. However, this directive does not cover the re-use of data that has a protected status and can therefore not be re-used as open data. This includes commercially sensitive data, data subject to confidentiality requirements, data protected by intellectual property rights, and individuals' personal data.

The DGA is meant to address this gap by setting the conditions under which the re-use of protected data held by PSBs (which can include both personal data as defined by the GDPR and non-personal data) is permitted. In practice, individuals, organizations, or companies will have the possibility to submit requests to PSBs for re-use of protected data, and the PSBs will have to decide whether they want to grant or refuse access to the data for re-use purposes.

In addition, PSBs will have to comply with a range of requirements, such as the obligations to:

- Refrain from granting exclusive rights relating to the re-use of protected data;
- Inform the public about the conditions for re-use of protected data (which must be non-discriminatory, transparent, proportionate, and objectively justified based on the sensitivity of the protected data);
- Implement technical measures to safeguard protected data that will be re-used (i.e., through anonymization, aggregation, or modification of protected data);
- Ensure that remote access to protected data only occurs within a secure processing environment (controlled by the PSB itself); and
- Impose confidentiality obligations on re-users of protected data.

The DGA's rules on re-use of protected data held by PSBs may create opportunities for a wide spectrum of sectors and industries that so far had only limited access to public sector information. In the area of medical research, for example, it is expected that new studies and trials will benefit from the ability to access (and use) existing data that is held by PSBs. There is a recent use case in France, where a public interest group named the French Health Data Hub has made re-use of medical data its main mission. Based on training data made available through the hub, a medical device company in France was able to develop technology that can help identify potential signs of skin cancer at an early stage.

Data Intermediation Services

Individuals and organizations are typically reluctant to make their (personal or non-personal) data available to others for various reasons, including potential abuse or competition concerns. The DGA attempts to address these concerns by enabling specialized organizations to provide DIS, with a view to facilitating the exchange of data. This can be achieved through technical, legal, or other means, such as by setting up data-sharing platforms between:

- Individuals or organizations that wish to grant access to or share personal or non-personal data (data subjects or data holders), and
- Those that want to have access to personal or non-personal data and re-use it for commercial or non-commercial purposes (data users).

The new DIS framework encourages voluntary data sharing and tries to increase trust among data subjects, data holders, and data users. Organizations that want to provide DIS services (in the form of data information management systems, data marketplaces, or data-sharing pools, for example) will have to comply with strict requirements to guarantee their independence and neutrality toward the parties that are exchanging data. For instance, the DGA requires DIS providers offering various types of services to ensure a strict separation between the DIS and any other services they provide to customers. Also, DIS providers will not be able to use the data exchanged via their data-sharing platform for their own purposes—other than improving their data-sharing facilities or detecting fraud.

Before offering their data-sharing services to potential customers, DIS providers will have to submit a notification to the competent supervisory authority (i.e., the authority of the EU Member State of their main establishment). Organizations that are not established in the European Union but wish to offer DIS within the European Union are required to designate a legal representative for DGA purposes in one of the EU Member States where they intend to offer their services.

The DIS concept may entice organizations to share, under strict conditions and via a neutral trustee, commercially sensitive information with non-profit organizations and even commercial companies. For example, a prominent telecommunications provider in Germany has set up a dedicated data-sharing platform for companies to upload, manage, and share production data for (process and supply chain) optimization purposes.

Data Altruism

The DGA also aims to encourage individuals and organizations to make their data available for general interest purposes (e.g., to improve health care systems, combat climate change, or optimize

the provision of public services) voluntarily and without reward. With that objective, the DGA introduces a new regime of "data altruism," which enables individuals and organizations to easily and safely authorize the altruistic use of their data by others.

Under this new regime, it will be possible to share data via recognized data altruism organizations (RDAOs) that pursue not-for-profit goals. These RDAOs will be subject to a range of strict requirements to make sure that individuals and organizations that make their data available can trust that the data will only be used to serve the public interest. For instance, RDAOs will have to comply with reporting and transparency obligations and implement specific measures to safeguard the rights of individuals and organizations sharing their data.

Organizations that want to become an RDAO will have to register with the competent supervisory authority in the relevant EU Member State. Like DIS providers, RDAOs without an establishment in the European Union will have to designate a legal representative for DGA purposes that is located in the European Union. Registered RDAOs will be able to use the European RDAO logo when communicating about their new activities and may be listed in the EU public record of RDAOs.

The DGA's provisions on data altruism are likely to fuel research activities in the European Union, particularly in the medical field. They will, for instance, enable individuals to make their health-related data available to researchers in a secure manner and for specific purposes that serve the public interest. For example, a German public health institute developed an application to help track the spread of COVID-19 in Germany. Thanks to citizens willing to share their health data (collected mainly through fitness bracelets or smart watches), the institute was able to paint a comprehensive picture of COVID-19 infection patterns. In another case, residents of the Spanish city of Barcelona agreed to share insightful data on the levels of noise, air pollution, temperature, and humidity in their city (collected through the use of sensors inside and outside their homes) with start-ups, cooperatives, and local communities.

Data Transfers

Transfers of personal data to recipients in countries outside the European Union are heavily restricted under the GDPR. The

DGA supplements the GDPR's data transfer regime by imposing restrictions on cross-border transfers of non-personal data.

The DGA requires PSBs, data users, DIS providers, and RDAOs to implement reasonable technical, legal, and organizational measures to prevent unlawful international transfers of or governmental access to non-personal data held in the European Union if that transfer or access would create a conflict with EU law or EU Member State law. This means that a "conflict assessment" will need to be conducted before the data can be transferred.

A foreign decision or judgment requiring transfer of or access to non-personal data held in the European Union can only be acted upon if it is supported by an international agreement, such as a mutual legal assistance treaty. If there is no such agreement and complying with the decision or judgment would risk putting the PSB, data user, DIS provider, or RDAO in conflict with EU law or EU Member State law, the data transfer or access can take place only if strict conditions are met (as set out in the DGA). Only minimum data should be provided in response to a request from a foreign court or authority and, when possible, the relevant data holders should be informed of the request.

In addition, the DGA imposes specific data transfer requirements on data users that wish to transfer non-personal protected data outside the European Union. They will have to:

- Inform, in advance, the relevant PSBs about their intention to transfer non-personal protected data outside the European Union;
- Commit to respect the specific conditions imposed by the PSBs;
- Submit to the jurisdiction of the EU Member State of the PSB that allowed the re-use of protected data; and
- In some cases, obtain data holders' authorization before transferring protected data.

Enforcement

Each EU Member State will have to designate a supervisory authority to oversee compliance with the DGA. These authorities will have the power to take enforcement action against organizations that do not comply with their DGA obligations. This includes

imposing administrative fines. The DGA leaves it up to the EU Member State authorities to determine the amounts of potential fines, taking into consideration the nature, gravity, and duration of the DGA violation, as well as any aggravating and mitigating circumstances.

The DGA also establishes a new expert group, the European Data Innovation Board (EDIB), which will be in charge of advising and assisting the EC in developing guidelines and best practices for PSBs handling requests for the re-use of protected data and to support DIS providers and RDAOs in complying with their obligations under the DGA. The EDIB is also tasked with providing guidance to EU Member States and their competent supervisory authorities and facilitating cross-border cooperation.

Interplay Between the DGA and the GDPR

The DGA regulates access to and re-use of data, both personal and non-personal, whereas the GDPR deals with processing of personal data only. Organizations that engage in sharing, accessing, or re-using personal data (or mixed sets of personal and non-personal data) under the DGA may therefore have to ensure compliance with the provisions of the GDPR as well. This means, for example, making sure that there is a valid legal basis for processing personal data (e.g., individuals' consent), complying with reporting requirements in case of a personal data breach, or implementing a data transfer tool if personal data is sent outside the European Union.

How Can the DGA Impact Businesses in the United States?

The DGA can be of relevance to any business that wants to make good use of the new data-sharing opportunities that the new law is expected to create. They would be well-advised to assess to what extent the DGA may apply to their activities and, if necessary, design a DGA compliance plan. Also, businesses in the United States that, for example, wish to offer DIS services or act as an RDAO will have to consider the DGA requirement to appoint a legal representative in the European Union. In addition, the DGA's data transfer restrictions may impact businesses in the United

States that are on the receiving end of non-personal data that is transferred by, for instance, a DIS provider in the European Union. In order to have access to that data, U.S. businesses may be asked to agree to contractual obligations and implement measures that aim to ensure the same level of data protection as under EU law.

Conclusion

In summary:

- The DGA introduces new rules to encourage sharing of personal and non-personal data across sectors;
- The DGA supplements other EU laws that regulate data use, such as the GDPR and the Digital Markets Act; and
- Businesses in the United States that receive non-personal data under the DGA might face data transfer restrictions.

Note

* The authors, attorneys with Alston & Bird LLP, may be contacted at alice.portnoy@alston.com and wim.nauwelaerts@alston.com, respectively.

Building Bridges: A Q&A About the UK's Extension to the EU-U.S. Data Privacy Framework

Annabel Gillham, Alex van der Wolk, and Dan Alam*

In this article, the authors discuss some of the key aspects and implications of the UK Data Privacy Framework extension.

It has been several months since the EU's adequacy decision[1] regarding the EU-U.S. Data Privacy Framework (DPF) entered into force. While we are already seeing challenges to the DPF in the European Union, the confirmation that the UK's "data bridge" or adequacy decision in respect of the DPF has been finalized will be welcome news to UK, U.S., and global businesses that routinely engage in cross-border data transfers.

From October 12, 2023, organizations subject to the UK General Data Protection Regulation (GDPR) have been able to rely on the DPF for cross-border transfers of personal information to DPF-certified companies without implementing other transfer mechanisms like the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses (UK Addendum), or Binding Corporate Rules (BCRs).

The UK government has also confirmed[2] that—like the European Union—its adequacy decision will also benefit personal information transferred to the United States under other transfer mechanisms, as companies can now onboard the decision into their transfer risk assessments.

This Q&A discusses some of the key aspects and implications of the UK DPF extension.

The Global Regulatory Developments Journal / January–February 2024, Vol. 1, No. 1, pp. 51–55.

ISSN 2995-7486.

When Can UK Companies Start Relying on the DPF?

The UK's regulations giving effect to the DPF came into force on October 12, 2023. From this date, the DPF can be used instead of the IDTA, the UK Addendum, or BCRs for transfers to DPF-certified companies that have opted in to the UK DPF extension.

How Do U.S. Companies Opt In to the UK Extension to the DPF?

Eligible U.S. companies have been able to certify under the UK DPF extension since July 17, 2023. The UK DPF extension is only available to companies that are part of the DPF (so a company must participate in the EU-U.S. DPF to partake in the UK DPF extension).

How Does the UK DPF Extension Affect Other Data Transfer Mechanisms?

While participation in the DPF is limited to U.S. companies subject to the investigatory and enforcement powers of the Federal Trade Commission and the U.S. Department of Transportation, other transfer mechanisms under UK law will continue to be valid for data transfers to the United States.

Both the U.S. and the UK government have stated that the DPF will be relevant to all transfers of personal information, regardless of the transfer tool used.

This means that the protections afforded by Executive Order (EO) 14086 (which limits U.S. surveillance activities to what is necessary and proportionate and established the Data Protection Review Court as a means of redress) will also apply to transfers made on the basis of the IDTA, UK Addendum, or BCRs. As the United States designated the United Kingdom as a qualifying state for the purposes of EO 14086 on September 18, 2023, these protections are already in place for UK personal information transferred to U.S. companies.

The Information Commissioner's Office (ICO) requires that companies subject to the UK GDPR complete a transfer risk assessment when relying on the UK IDTA, UK Addendum, or BCRs to transfer personal information to a non-adequate country. Following

that assessment, the company must determine if mitigation measures are required to reduce the risk of the proposed transfer. Following the UK DPF extension, when transferring personal information to a U.S. company that is not certified by the DPF, the company will be able to also benefit from the commitments made by the United States under EO 14086 and the UK government's assessment of these commitments.

When transferring personal information to a DPF-certified company, transfer risk assessments or mitigation measures are not required. This position aligns with the EU approach, according to the European Data Protection Board's opinion following the DPF.[3]

What Additional Considerations Are There for Transferring Sensitive and Criminal Information When Using the DPF?

The definition of "sensitive information" in the UK DPF extension does not specify all of the types of information in the UK GDPR that are subject to additional requirements (it omits genetic and biometric information, as well as information about an individual's sexual orientation and criminal offense information). However, the definition does include "any other information received from a third party that is identified and treated by that party as sensitive." The ICO and the UK government have stated that organizations will need to identify such information as sensitive when sending it to DPF-certified organizations.

In its opinion[4] published after the UK DPF extension was finalized, the ICO has also raised a concern that the protections set out in the UK Rehabilitation of Offenders Act 1974 (which limit the use of information relating to historic criminal convictions) is not provided for in the DPF. UK companies transferring such information to the United States should ensure that limitations are placed on the use and retention of such information in a manner that complies with UK law.

Are There Risks to Relying on the UK DPF Extension?

The UK government is required to review the UK DPF extension every four years from the date it entered into force. However, if it

becomes aware of a significant change in the level of data protection provided under the DPF, it must amend or revoke its adequacy decision as necessary.

The DPF is already under challenge in the European Union, as an individual in France has brought an action before the General Court of the European Union for annulment and immediate suspension against the DPF (on the basis that the DPF violates the EU Charter of Fundamental Rights). The EU Charter of Fundamental Rights no longer applies under UK law and the adequacy finding from the United Kingdom will not be directly affected by any such challenge.

Will the United Kingdom Be Creating More "Data Bridges"?

The UK government has indicated its intention of doing so. Following the UK DPF extension, the European Union and the United Kingdom now recognize the same countries as adequate. The UK government has also published[5] a list of priority destinations to recognize as adequate, which, in addition to the United States, includes Australia, Brazil, Colombia, the Dubai International Financial Centre, India, Indonesia, Kenya, and Singapore.

The UK's new data protection bill, which is still making its way through the UK legislative process, proposes to change the test on which the UK government can recognize a country as adequate from "essentially equivalent" to "not materially lower" data protection standards. This suggests that the United Kingdom may seek to recognise more countries as adequate through additional data bridges.

What About the EU'S Adequacy Decision for the United Kingdom?

Data transfers from the European Union to the United Kingdom are currently covered by the adequacy decision granted by the European Commission in 2021. The European Commission's adequacy decision contains a sunset clause, which means that it will expire on June 27, 2025, if it is not renewed. To date, the UK government has maintained[6] that the proposed reforms to its data protection laws will not affect its adequacy status.

Notes

* The authors, attorneys with Morrison & Foerster LLP, may be contacted at agillham@mofo.com, avanderwolk@mofo.com, and dalam@mofo.com, respectively. Lewis Ball, a trainee solicitor, assisted in the preparation of this article.

1. https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

2. https://www.gov.uk/government/publications/uk-us-data-bridge-supporting-documents/uk-us-data-bridge-explainer#:~:text=Supporting%20this%20decision,national%20security%20purposes.

3. https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf.

4. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/09/opinion-on-uk-government-s-assessment-of-adequacy-for-the-uk-extension-to-the-eu-us-data-privacy-framework/.

5. https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation#uk-adequacy.

6. https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation.

China Publishes Draft Rules to Ease Data Export Compliance Burden

Lester Ross, Kenneth Zhou, and Tingting Liu*

In this article, the authors examine the draft Provisions on the Regulation and Promotion of Cross-Border Data Flows issued recently by the Cyberspace Administration of China.

The Cyberspace Administration of China (CAC) has issued the draft Provisions on the Regulation and Promotion of Cross-Border Data Flows (draft Provisions),[1] just one year after China's data export security management framework was formally established.[2] The fact that CAC released the draft shortly before China's week-long National Holiday and set a short period for public comment suggests that CAC intends to finalize the draft and promulgate the Provisions soon.

The current data export compliance regime is underpinned by three alternative pillars: a mandatory data export security assessment when certain thresholds are crossed, personal information (PI) standard contract clauses (SCC) filing, or PI protection certification (PIPC).

The draft Provisions are a short document, consisting of only eleven clauses. Nonetheless, if adopted in their current form, they would significantly soften the current data export rules by:

1. Raising the thresholds for triggering data export filing obligations;
2. Establishing exemptions for common data export scenarios;
3. Clarifying that certain PI/data would no longer be subject to export filing requirements; and
4. Establishing a more flexible policy space for exercising negative-list management in free trade zones (FTZ) where many foreign-invested enterprises are registered.

The draft Provisions may be understood as a response by Chinese officials to concern over the tremendous administrative,

The Global Regulatory Developments Journal / January–February 2024, Vol. 1, No. 1, pp. 57–61.

ISSN 2995-7486.

commercial, and human resource burdens that the existing regulations impose on both domestic and international business communities as well as the burden on cybersecurity officials tasked with regulatory implementation. Pending finalization, they constitute a welcome development that will promote cross-border trade and investment amid China's sluggish economy.

Raised Thresholds

- Annual PI export involving fewer than 10,000 individuals would no longer be subject to a mandatory data export security assessment, SCC filing, or PIPC requirements.
- Annual PI export involving more than 10,000 but fewer than 1 million individuals would no longer be subject to a mandatory data export security assessment, replaced by a less burdensome SCC filing with the relevant provincial CAC or a PIPC.

Under the current rules, a data processor, that is, a company or other entity operating in China, is subject to a mandatory CAC-led data export security assessment when the "1 million/100,000/10,000" thresholds are met. If the thresholds are not met, an SCC filing or PIPC is required. The current thresholds for determining whether a data processor is subject to a mandatory security assessment are as follows:

- Processes PI of more than 1 million individuals; or
- Cumulative PI of 100,000 individuals or Sensitive PI of 10,000 individuals have been exported since January 1 of the previous year.

While the mandatory CAC-led security assessment also applies to data processed by critical information infrastructure operators (CIIOs) and Important Data, as a practical matter, multinational corporations (MNCs) are unlikely to be designated as CIIOs, and they are unlikely to process Important Data except in the instance where the number of individuals whose PI is processed exceeds 1 million, in which case the PI is deemed to constitute Important Data.

Currently, CAC nationwide has approved mandatory security assessments for only a few dozen large-scale companies that crossed

the "1 million/100,000/10,000" thresholds, while many others remain in the queue. No data is publicly available on how many companies have crossed the thresholds, how many have chosen to file for review of their security assessments, or how many have been rejected. Even companies that have not crossed the "1 million/100,000/10,000" thresholds are subject to either an SCC filing or a PIPC requirement if they export any PI overseas. Such requirements cast a wide net sweeping in large numbers of MNCs that exchange essential business and governance information with overseas affiliates or counterparts.

Moreover, even an SCC filing that triggers a self-assessment by the company or a PIPC that is outsourced to a third-party accredited institution is financially and administratively burdensome. Raising the filing thresholds will exempt many companies from the compliance requirements under the current data export regime.

Exempted Data

Data export security assessment, SCC filing, and PIPC would also not be required if:

- Data export is necessary for the execution and performance of a contract to which an individual is a party, such as the cross-border purchase of goods, cross-border fund transfers, air tickets or hotel reservations, and visa processing;
- Data export is related to a company's internal employee data and necessary for human resources management in accordance with the company's labor policies and rules formulated on the basis of a law, regulation or collective bargaining contract; or
- Data export is necessary for the protection of personal safety, health, or property security in an emergency.

The current compliance regime does not distinguish among the types of data that are transferred overseas. In fact, except for those MNCs that have completely localized their data sets in China, many MNCs currently share customer data and employee data with their overseas head offices to process cross-border transactions and manage human resources or simply for record keeping purposes, on a globally integrated system. This means that under the current compliance regime, MNCs in theory are subject to at least an SCC

filing or PIPC obligation, even if no mandatory security assessment threshold is crossed.

The data exemptions also may ease the burden facing cross-border e-commerce service providers, travel service providers, and retail businesses that export customer data, as well as MNCs that maintain global employee data processing systems.

Further Clarification

- Unless specifically categorized as Important Data by government through notification or announcement, data processors would not need to treat their data as Important Data, which is subject to more stringent protection requirements than ordinary data, for purposes of a mandatory data export security assessment.
- Outbound transfers of data not containing PI or Important Data that is generated in international trade, academic collaboration, cross-border production, or marketing and sales activities would no longer be subject to a data export security assessment, SCC filing, or PIPC.
- Data not collected or generated in China would not be subject to a data export security assessment, SCC filing, or PIP certification obligation.

The scope of Important Data has been a persistent concern for MNCs, as any export of Important Data automatically triggers a mandatory security assessment, regardless of whether the relevant thresholds have been met. With the new Provisions, MNCs will no longer need to worry that the data they process will fall in the category of Important Data unless the data is specifically classified as Important Data. This clarity will create certainty and ease compliance burdens. MNCs handling data generated from overseas, such as personal information of foreign nationals, would also face less onerous compliance burdens.

Negative List in Free Trade Zones

Critically, administrative responsibility in some instances will be transferred from CAC to more investment-friendly bodies. Pilot FTZs will be authorized to establish a "Negative List" regime and

all future data export activities not covered in such Negative Lists would no longer be subject to data export security assessment, SCC filings, or PIP certification requirements.

Conclusion

The draft Provisions are a response to the State Council's proposal to establish a security management mechanism to facilitate data cross-border flows, one of the measures to further optimize the environment for foreign investment.

Unlike the European Union, which recognizes the value of cross-border data transfers and has been prepared to negotiate data protection agreements to ensure that PI and other data can be exported provided that the recipient jurisdiction provides protections equivalent to the General Data Protection Regulation, China seems to have imposed a rigid data export control regime focusing on national security considerations. The draft Provisions indicate a willingness to relax the burdens that the current regime has created.

The draft Provisions, if adopted in their current form, will exempt a large number of companies exchanging information with overseas affiliates and counterparts in normal business scenarios from data export filing requirements, unless they export Important Data, the scope of which has been limited, or the PI of a large number of individuals. This will significantly ease the burden facing a typical MNC operating in China, and will be welcomed by the business community domestically and internationally.

Notes

* The authors, attorneys with Wilmer Cutler Pickering Hale and Dorr LLP, may be contacted at lester.ross@wilmerhale.com, kenneth.zhou@wilmerhale.com, and tingting.liu@wilmerhale.com, respectively.

1. http://www.cac.gov.cn/2023-09/28/c_1697558914242877.htm.

2. The Measures for Data Export Security Assessment took effect as of September 1, 2022, followed by the Announcement to Implement Personal Information Protection Certification and the Measures on the Standard Contract for Personal Information Export.

Get Ready for India's New Data Privacy Law

Cynthia J. Rich*

In this article, the author provides an overview of the Act's key requirements of India's new Digital Personal Data Protection Act.

After more than five years of debate and legislative proposals, India has finally enacted an omnibus data privacy law. The Digital Personal Data Protection Act of 2023 (the Act) establishes a high-level legal framework that regulates the processing of personal data in India and processing outside India that is related to offering goods or services to individuals in India. Implementing regulations will be issued in the next few months and provide more specifics on how the obligations under the Act must be implemented. The government has not yet announced the date the law will take effect but, based on public statements by government officials, the government would like the law to take effect within six months of its enactment in August 2023. Once the Act takes effect, the current privacy rules issued under Section 43A of the Information Technology Act will no longer be in effect.

While the Act imposes the key privacy obligations commonly found in data privacy laws around the world, some of these obligations are limited to certain data controllers, referred to as "Data Fiduciaries" or classes of Data Fiduciaries. There are other aspects of the law that set it apart from other data privacy laws, including the EU's General Data Protection Regulation (GDPR). In particular, the Act does not restrict cross-border transfers of personal data, although it does provide the government with the ability to do so in the future.

More significantly, like the Philippine data protection law, the Act specifically protects the Indian outsourcing industry by ensuring that foreign personal data sent to outsourcing providers in India for data processing are not subject to multiple and potentially conflicting data privacy requirements.

In the coming months, companies that process personal data of individuals located in India will need to ensure that their privacy practices conform to the new Indian requirements. Enforcement will begin after the implementing regulations are issued. In late

The Global Regulatory Developments Journal / January–February 2024, Vol. 1, No. 1, pp. 63–69.

ISSN 2995-7486.

October, the Minister for Electronics and Information Technology announced that the government would be releasing soon its draft implementing regulations for a 45-day public consultation before submitting them to Parliament for approval.[1]

This article provides an overview of the Act's key requirements.

Application

The provisions of the Digital Personal Data Protection Act apply to the processing of digital personal data:

- In India where:
  - The personal data are collected in digital form; or
  - The personal data are collected in non-digital form and digitized subsequently; and
- Outside India, if such processing is connected to any activity related to the offering of goods or services to individuals in India.

The Act does not apply to personal data processed by an individual for any personal or domestic purpose and personal data that are made or caused to be made publicly available by the individual or any other person who is under any obligation under any law in force in India to make such personal data publicly available. Personal data are defined as any data about an individual who is identifiable by or in relation to such data.

Outsourcing

Processing of personal data of individuals not located in India that is pursuant to a contract entered into with any entity outside India by an entity based in India is not subject to the obligations under the Act imposed on Data Fiduciaries (including Significant Data Fiduciaries), the cross-border transfer rules, or individual rights obligations; however, the security provisions do apply.

Data Fiduciaries

The Act imposes obligations on Data Fiduciaries, individuals, or entities that determine the purposes and means of processing

personal data. In addition, the government, by way of a notification, may designate any Data Fiduciary or class of Data Fiduciaries as a "Significant Data Fiduciary" on the basis of an assessment of factors, including:

- Volume and sensitivity of personal data processed;
- Risk of harm to the individual;
- Potential impact on the sovereignty and integrity of India;
- Risk to electoral democracy;
- Security of the state;
- Public order; and
- Other factors that it may consider necessary.

Legal Bases for Processing

Data Fiduciaries may process the personal data of individuals for a lawful purpose (defined as any purpose which is not expressly forbidden by law) for which individuals have consented or for certain "legitimate purposes." Legitimate purposes include uses such as for:

- The specified purpose for which individuals have voluntarily provided their personal data to the Data Fiduciary and where the individuals have not indicated to the Data Fiduciary that they do not consent to the use of their personal data;
- Fulfilling any obligation under any law in force in India on any entity to disclose any information to the government;
- Compliance with any judgment or decree or order issued under any law in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law in force outside India; or
- Responding to a medical emergency involving a threat to the life or immediate threat to the health of the individual or any other individual.

Consent is defined as being free, specific, informed, unconditional, and unambiguous with a clear affirmative action that signifies an agreement to the processing of personal data for the specified purpose and limited to such personal data as are necessary for such specified purpose. Individuals have the right to withdraw consent at

any time, with an ease similar to that with which such consent was given. Individuals may give, manage, review, or withdraw consent through a "Consent Manager" (an entity that is accountable to the individuals and acts on their behalf). Every Consent Manager must be registered with the Data Protection Board, the data protection authority of India.

Notice

At the time of or prior to requesting consent from individuals, a Data Fiduciary must provide to individuals an itemized notice in clear and plain language containing a description of the types of personal data to be collected, the purposes for the processing, and the manner in which individuals may exercise their rights. Where individuals have consented to the processing of their personal data prior to the commencement of the Act, the Data Fiduciary must give a similar notice to them as soon as reasonably practicable. The Data Fiduciary must give individuals the option to access the contents of the notice in English or any of the 22 languages specified in the Eighth Schedule to the Indian Constitution.[2]

Individual Rights

Access, correction, and erasure rights must be provided. The Act does not prescribe a time frame for responding to rights requests or provide exceptions for provision of access or correction. In connection with erasure requests, individuals may request erasure of their data where they are no longer necessary for the purpose for which they were processed unless retention is required for a legal purpose. Individuals also have the right to a readily available redress mechanism provided by the Data Fiduciary or the Consent Manager.

Security

Data Fiduciaries must implement appropriate technical and organizational measures to ensure effective adherence to the provisions of the Act. Every Data Fiduciary must protect personal data in its possession and under its control, including in respect of any

processing undertaken by it or on its behalf by a processor, by taking reasonable security safeguards to prevent personal data breaches.

Data Breach Notification

In the event of a personal data breach, the Data Fiduciary must notify the data protection authority and affected individuals. The Act does not specify the notification trigger or the reporting time frame.

Disclosures to Processors

A Data Fiduciary may only engage a processor to process personal data on its behalf for any activity related to offering of goods or services to individuals under a valid contract.

Cross-Border Transfers

The government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to a country or territory outside India. In addition, the Act does not restrict the applicability of any law in force in India that provides for a higher degree of protection for or restriction on the transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or classes of Data Fiduciaries.

Additional Obligations Imposed on Significant Data Fiduciaries

Significant Data Fiduciaries must:

- Appoint a Data Protection Officer (DPO), based in India, who will represent the company. The DPO must be an individual who is responsible to the Board of Directors or a similar governing body of the company. The DPO will be the point of contact for the dispute resolution mechanism;
- Appoint an Independent Data Auditor who will evaluate the company's compliance with provisions of this Act; and

- Undertake other measures, including Data Protection Impact Assessments and periodic audits in relation to the objectives of this Act, as may be prescribed in the implementing regulations.

Data Retention

Unless retention is necessary for compliance with any law in force, a Data Fiduciary must erase personal data when the individual withdraws consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier, and require the processor to erase any personal data provided to it by the Data Fiduciary for processing.

Complaint Resolution

Every Data Fiduciary must have in place a procedure and effective mechanism to address the grievances of individuals.

Processing Personal Data of a Child

Before processing the personal data of a child (i.e., any individual under the age of 18), the Data Fiduciary must obtain verifiable parental consent. A Data Fiduciary must not undertake processing of personal data that is likely to cause harm to a child and must not undertake tracking or behavioral monitoring of children or targeted advertising directed at children.

Exceptions

In addition to outsourcing, certain other processing activities are exempted from all but the security provisions of the Act, such as processing in the interest of prevention, detection, investigation, or prosecution of any offense or contravention of any law, processing that is necessary to enforce a legal right or claim, or processing that is necessary for a corporate merger or sale.

Data Protection Board/Penalties

The Act provides for the creation of the Data Protection Board of India, an independent body responsible for enforcement of the Act. The Board will have the authority to impose financial penalties ranging from INR 10,000 to 2.5 billion (USD 1,200 to 30.2 million). In particular, failure of a Data Fiduciary to take reasonable security safeguards to prevent a personal data breach is punishable by a penalty up to USD 30.2 million (250 crore); failure to notify the Data Protection Board and affected individuals of a personal data breach is punishable by a penalty up to USD 24 million (200 crore).

Notes

* Cynthia J. Rich, a senior privacy advisor at Morrison & Foerster LLP, may be contacted at crich@mofo.com.

1. As of November 28, 2023, the draft implementing regulations have not yet been released for public consultation.

2. The 22 languages are Assamese, Bengali, Bodo, Dogri, Gujarati, Hindi, Kannada, Kashmiri, Konkani, Maithili, Malayalam, Manipuri, Marathi, Nepali, Odia, Punjabi, Sanskrit, Santhali, Sindhi, Tamil, Telugu, and Urdu.

Driverless in Dubai: Autonomous Vehicle Regulation Advances in the United Arab Emirates

Christopher R. Williams and Amelia Bowring*

In this article, the authors explain that the United Arab Emirates is resolutely positioning itself as a leader in innovation and technology, aspiring for Dubai to be the model city of the future.

In line with Dubai's Autonomous Transportation Strategy (the Strategy), on April 14, 2023, Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the United Arab Emirates and Ruler of Dubai, introduced legislation to provide a legal basis for the Strategy being adopted as Law No. (9) of 2023 on regulating the operation of autonomous vehicles in Emirate of Dubai (the Law).

The UAE is resolutely positioning itself as a leader in innovation and technology, aspiring for Dubai to be the model city of the future, and the introduction of the Law demonstrates the country's commitment to the same.

The Law aims to regulate the operation of autonomous vehicles in accordance with international best standards and attract investment into Dubai in respect of related activities. Among others, a key aim of the Strategy is to transform 25 percent of transportation in Dubai to autonomous mode by 2030, with an estimated resulting saving of AED 22 billion in annual economic costs.

Powers Granted

The Law grants Dubai's Road Transport Authority (the RTA) wide discretionary powers in respect of the governance of autonomous vehicles, including:

1. Determining the types of vehicles to be made autonomous;
2. Selecting locations in Dubai where autonomous vehicles will be permitted;

The Global Regulatory Developments Journal / January–February 2024, Vol. 1, No. 1, pp. 71–73.

ISSN 2995-7486.

3. Licensing autonomous vehicles;
4. Planning to facilitate investment; and
5. Creating the infrastructure required to operate autonomous vehicles in Dubai.

In order to operate an autonomous vehicle in Dubai, the following must be granted: (1) an autonomous vehicle license, and (2) permission from the Director General of the RTA for the proposed operator to partake in activities related to autonomous vehicles. Furthermore, the following criteria must be met for a vehicle to be licensed as an autonomous vehicle by the RTA:

1. The initial registrant of the vehicle must have prior approval for the particular type of vehicle in Dubai;
2. The vehicle should be registered in the country of origin or exporting country and proven that it has been used on public roads allocated for the category and type of autonomous vehicle in such country;
3. The vehicle must pass all RTA technical examinations;
4. The vehicle must appropriately read traffic signs and handle road priorities;
5. The vehicle should meet the criteria of standards of safety and security as set out in the RTA's approved guide;
6. The vehicle must conform with the specification approved in the UAE;
7. An insurance company licensed in the UAE as determined by the RTA's Director General should insure the vehicle; and
8. Any other conditions that may be determined by the RTA's Director General from time to time should be met.

The procedures for licensing an autonomous vehicle that meet the above conditions are still to be decided by the RTA's Director General.

Obligations

The Law also sets out responsibilities relating to not only the operator of an autonomous vehicle but also passengers of such vehicles, who must also comply with certain rules when being driven by an autonomous vehicle. The Law also sets out certain

responsibilities placed on the owner/operator of such vehicles and those parties who are responsible for the sale and distribution of the same in Dubai. Consequently, owners, operators, passengers, and distributors are all subject to certain obligations pursuant to the Law. In addition, the Law also restricts the way in which autonomous vehicles are sold insofar as sales to a licensed operator are only permitted through the relevant agent and the transfer of ownership from one operator to another may only occur following prior approval of the RTA.

Anyone who violates the Law shall be subject to a fine of no less than AED 500 and no more than AED 20,000, which may be doubled in the event of repeat violations within the same year with a maximum fine set at AED 50,000.

Conclusion

Dubai is planning to soon launch autonomous taxi services that are due to be delivered by Cruise, in exclusive partnership with RTA with the first set of self-driving taxis being custom built on the foundation of the Chevrolet Bolt.

Dubai aims to deploy 4,000 self-driving taxis by 2030, and Cruise has been designated as the exclusive robotaxi service provider in the city until 2029. This project will make Dubai the first non-U.S. city to commercialize Cruise's self-driving cars.

The introduction of autonomous vehicles will not only alleviate traffic congestion but also reduce the number of road traffic accidents and harmful emissions, making Dubai an even more attractive destination for tourism and business.

Note

* The authors, attorneys with Bracewell LLP, may be contacted at chris.williams@bracewell.com and amelia.bowring@bracewell.com, respectively.

Published six times annually, *The Global Regulatory Developments Journal* explores and analyzes the most significant global regulatory developments taking place in the European Union, the United Kingdom, Canada, the United States, Latin America, Asia, and elsewhere around the world. *The Global Regulatory Developments Journal* covers topics of interest to international attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and others interested in global regulatory developments, with an emphasis on the hottest topics in international regulation today: Privacy and Cybersecurity, Global Finance and Investments, Climate and Energy, Technology, and International Labor and Employment.

fastcase FULL COURT PRESS

ISSN 2995-7486