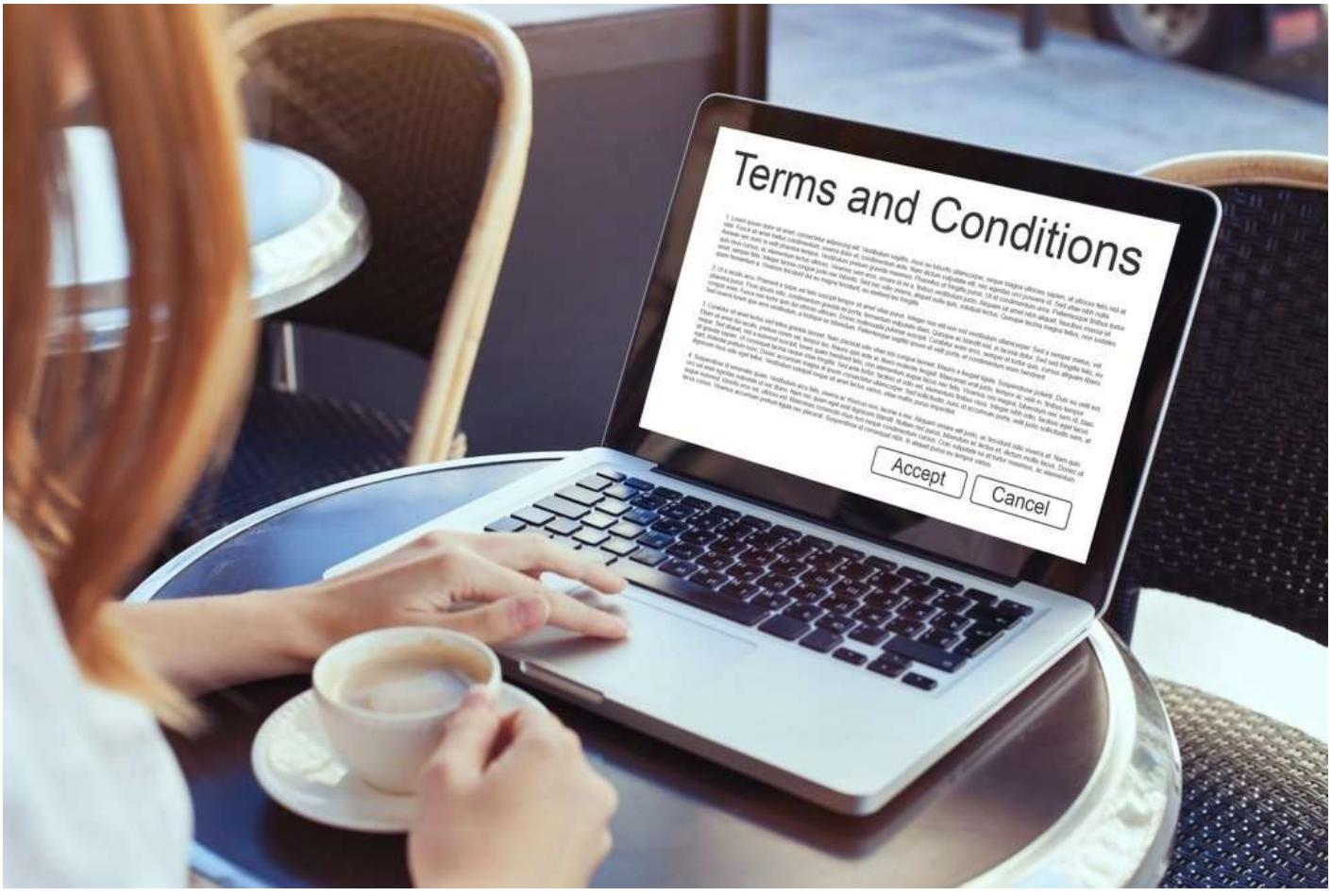
Data Licensing—Tips and Tactics

by Daniel Masur — September 5, 2018 in Data Privacy, Featured



Compliance Considerations when Obtaining Data from a Third Party

Companies often claim that data is one of their most precious assets, but they rarely treat it as such. Mayer Brown Partner Dan Masur discusses The Big Data Paradox, and in this article, outlines a number of issues inherent in ensuring regulatory compliance when obtaining data from an outside source.

with co-authors Brad L. Peterson and Corina Cercelaru

Companies obtain data from an increasing number of sources. Some of these sources are under contracts titled "data license agreements," but most are under other types of agreements. Those other agreements might include subscription agreements, website terms of use, outsourcing agreements, purchase and sale agreements, alliance agreements and other commercial agreements.

Data acquired from third parties generally come with license and use restrictions and may come with restrictions that attach to personal data. In some cases, the license terms associated with the data are subject to significant negotiation. In other cases, however, a company accepts license terms with little thought as to whether they are aligned with the anticipated handling and use of the data.

To ensure compliance with applicable license terms, each item of licensed data must be linked to its source and to the specific terms on which the data was obtained. Unfortunately, data is often not tracked at all, or the data provenance is lost when the data flows into a database or from one database into another. The danger, of course, is that data is used in ways and for purposes not contemplated by the license. This can result in license breaches, privacy law violations, intellectual property violations and regulatory compliance failures.

Even keeping track of data can be challenging. Software often has a "software fingerprint" and may even be reporting on its use. By comparison, it may be costly or even impossible to identify all of the locations where licensed data is being stored or used. Thus, without advance planning and technology, it can be difficult or even impossible to demonstrate that a company's data use is consistent with the terms of the applicable license grant and may expose it to significant liability in the event of an audit.

Tracking data provenance and its related restrictions is new to many companies, and, like many new areas, it requires that a company develop policies and procedures. When a company is licensing data from a third party, there are important considerations which, when properly managed, can lead to better data licenses. The following are important issues to be addressed when obtaining data from a third party.

Licensed Data

The core provisions of a data license agreement define the data that is being licensed, including the manner and frequency with which the data will be provided/updated, how current the data will be (that is, whether the data will be provided on a "real-time" or close to "real-time" basis), the format in which the data will be delivered and the mechanism of delivery. Such terms may include the use of encryption and a secure delivery mechanism, designated communications technology platforms and specific hardware or software configuration requirements. These provisions vary from a general license that may be accessible to the licensee during the license term to a specific license — for example, to market data on specific assets within a specific time after the market event occurs.

Users

The data license must also establish who is permitted to use the licensed data. For example, the license agreement may identify the people who are permitted to use the data or the devices on which the data may be used or may specify the maximum number of such users or devices. The licensee should be sure that any such restrictions are consistent with its anticipated use of the data. In addition, given the complex structures of many corporations, consider making clear that data use is not restricted to the entity executing the license and that the licensed data may be used by affiliates of that entity. Also, to the extent a company uses third-party contractors, it may be important to provide that the licensed data may be used by such third-party contractors in performing services on behalf of the licensee.

Finally, depending on the business model of the licensee, it may be important to provide that the licensed data may be accessed and used by regulators or customers of the licensee and its affiliates. Of course, it is also important to flow down to the affiliates, third-party contractors (and their subcontractors) and customers any license restrictions on the use of such data.

To the extent relevant, the data license agreement should also address the issue of exclusivity. Most data license agreements are nonexclusive, where the licensor has the same rights to the data as the licensee and can also license the data to other third parties. Less often, a licensee may require an exclusive license to the data, which will only grant rights to the data to the licensee, not allowing

use or access by any other parties, including the licensor. A sole license is another option. A licensee may seek a sole license if it does not want the data to be licensed to other third parties, but to allow the licensor to continue to access and use the data.

Purpose

In some cases, data is licensed for a specific purpose and only for that purpose. For example, in the case of a bank, a customer may provide data for the purpose of opening and maintaining an account, obtaining a mortgage or other loan, engaging in a corporate transaction, facilitating the completion of required "know-your-customer" checks, etc. However, in many cases, the data finds its way into other databases, where it is unwittingly used for new or different purposes. It is thus important for the licensee to seek to include in the data license (which, in this example, might be a customer agreement) all of the possible purposes for which the data may be used, including, to the extent possible, possible future uses. If the purpose clause is not as general with regard to those possible future uses, compliance processes are needed to avoid a possible license breach.

Location Restrictions

For companies that operate in many locations, it is important to focus on where the data can be stored, accessed and used. For example, the proffered data license may limit storage, access and use to the United States. If storage, access or use of the data outside the United States is contemplated now or may be in the future, make that clear in the license agreement.

Privacy and Security

Given the proliferation of data protection laws and the current focus on data privacy and cybersecurity, it is important to address in the data license the nature and sensitivity of the data to be provided, the steps the licensee is obligated to take to protect the data and the licensee's potential liability if a data breach occurs.

Quality

Licensors often seek to disclaim any representation or warranty with respect to the completeness, accuracy, timeliness or utility of the licensed data. A licensee may see the following disclaimers, particularly where the data is licensed to many licensees under a form agreement or where the licensor is not in the business of licensing the specific type of data:

- The data is licensed “as is” and “as available” and the licensor does not assume any responsibility for the use of the licensed data;
- The licensor provides no representations or warranties about the accuracy, completeness, authenticity, usefulness, timeliness, reliability, appropriateness or sequencing of the data; or
- The licensor does not represent or warrant the data or access to it will be uninterrupted or error-free, or that errors will be

Carefully consider whether, given the nature and anticipated uses of the data, the disclaimers are acceptable. If the licensor resists a requested warranty on the theory that the licensor’s data is what it is, and has not been scrubbed, consider adding a knowledge or materiality qualifier.

Rights

It goes without saying that the licensor cannot grant the licensee broader rights in the data than the licensor possesses. So, it is important for the licensee to satisfy itself through due diligence and to document in the license agreement that the licensor possesses and is able to grant the licensee all of the rights the licensee requires to use the data for the anticipated purposes. This is especially true with respect to personal data where, in many cases, the licensor is not obtaining the personal data directly from the individual data subject. If notice to or the consent of the individual data subject is required, it is important that the licensor represents and warrants that it gave such notice or obtained such consent or that it obtained adequate assurances that the entity providing the data did so. In some cases, the parties will also need a mechanism that makes licensees aware if individual data subjects withdraw consent.

Term and Termination

Finally, it is important to define when your rights with respect to the data begin and end. Often, data is licensed for a limited subscription term, with the understanding that it will be returned or destroyed at the end of the subscription term. However, for practical reasons, the licensee may require a perpetual license for data previously received and incorporated in the licensee’s systems. Given the proliferation of corporate databases and the ease with which data moves from one to another, it may be difficult or even impossible to track down the data. In addition, to the extent the data has been co-mingled with other data sets, it may not be feasible for the licensee to extract or stop using the data. Finally, many companies, such as financial institutions, will require a perpetual license to meet regulatory or control obligations to maintain the underlying data for decisions and actions.

This article originally appeared in the Mayer Brown e-book, Technology Transactions: Thriving in an Age of Digital Transformation. It is republished here with permission.

Tags: data governance KYC

Previous Post

Miller & Chevalier Releases Inaugural 2018 Europe-Caucasus-Asia Corruption Survey

Next Post

TRACE: Antitrust: Price-Fixing and Collusion

Daniel Masur

Dan Masur is the Partner-in-Charge of Mayer Brown's Washington, D.C. office and a leader of its Technology Transactions practice. For more than 20 years, Dan has represented national and international clients in a broad range of on-shore, near-shore, and offshore information technology and business process sourcing transactions involving global and niche outsourcing providers, offshore captives and various hybrid structures. In addition, in recent years, Dan has represented clients in cutting-edge arrangements with digital service providers involving cloud, "big data," "as-a-service," "internet of things," robotic process automation, artificial intelligence and blockchain. Dan also deals on a regular basis with data privacy, data protection and cybersecurity issues. Dan has represented established and emerging companies in many different industries, including banking, aerospace, defense contracting, electronic commerce, financial services, pharmaceuticals, insurance, health care, life sciences, chemicals, consumer products, manufacturing, oil/gas, real estate, forestry products, telecommunications, information technology, and utilities/electrical power. Dan is recognized as one of the leading lawyers in the highly specialized outsourcing field by *Chambers Global* ("1" ranking in Outsourcing), *Chambers USA* ("1" ranking in "Nationwide: Outsourcing" and "DC: Technology & IT Outsourcing"), *Legal 500* (recognized in "Technology Outsourcing") and *Best Lawyers in America* (recognized in Information Technology Outsourcing). Dan joined Mayer Brown in 1997. From 1994 to 1997, he served as Vice President and General Counsel of I-NET, Inc., a rapidly growing provider of information technology, telecommunications and outsourcing services. Prior to I-NET, Dan was a partner in another Washington DC firm. Dan is a frequent speaker and presenter at industry and legal conferences on sourcing and technology subjects.

Related Posts

Is Your Data Supply Chain Ethical? Don't Restrict Due Diligence to Physical Operations.

by Andrew Blasi and Nicholas Diamond JUNE 15, 2021

Both your company's data supply chain and its physical version have fundamentally similar business risks. Given the consequences of unethical...

TrustArc: 2021 Global Privacy Benchmarks Report

by Corporate Compliance Insights JUNE 7, 2021

TrustArc, the leader in data privacy management and automation has released its 2021 TrustArc Global Privacy Benchmarks Report. Now in...

The Trump Administration Allowed an Estimated $84B in EIDL and PPP Fraud. Now Congress Is Revamping Oversight.

by Al Leiva, Jennifer Summa and Thomas Barnard MAY 26, 2021

The Biden administration, in a March memo, estimated EIDL and PPP fraud has totaled $84 billion to date. Numerous federal...

MoneyGram Agrees to Pay OFAC $34K for Sanctions Violations

by Michael Volkov MAY 20, 2021

OFAC's recent enforcement action against MoneyGram underscores organizations' need for robust screening to ensure AML compliance and prevent sanctions violations....

Join the conversation!

Get the latest GRC News, Views, Jobs & Events Delivered to Your Inbox

What's your current role? *

- ◯ Compliance Officer
- ◯ Risk Manager
- ◯ Info-sec / Data Privacy / Cybersecurity
- ◯ Internal Auditor
- ◯ C-Suite or Board Member
- ◯ Legal Professional / General Counsel
- ◯ Human Resources
- ◯ Consultant
- ◯ Media / Author / Advertiser
- ◯ Other

Business Email*

Country of Residence*

Subscribe to the Newsletter

☐ In addition to the newsletter, I understand I may also receive occasional information about webinars, events or GRC resources. I can unsubscribe from the newsletter or special offers at any time. Privacy policy available at link in footer.*

Submit

Jump to a Topic

AML anti-corruption Artificial Intelligence/A.I. automation banks board of directors board risk oversight bribery CCPA/California Consumer Privacy Act Cloud Compliance communications management Coronavirus/COVID-19 corporate culture crisis management culture of ethics cyber crime cyber risk data analytics data breach data governance decision-making diversity DOJ due diligence ESG fcpa enforcement actions financial crime GDPR GRC HIPAA information security KYC machine learning

monitoring regtech reputation risk risk assessment Sanctions SEC social media risk technology third party risk management tone at the top training whistleblowing

Search...

Privacy Policy

*Founded in 2010, CCI is the web's premier global **independent** news source for compliance, ethics, risk and information security.*

Got a news tip? Get in touch. Want a weekly round-up in your inbox? Sign up for free. No subscription fees, no paywalls.

Follow Us

Category

CCI Press
Compliance
Compliance Podcasts
Cybersecurity
Data Privacy
EBooks
Ethics
FCPA
Featured
Financial Services
Fraud
Governance
GRC Vendor News
HR Compliance
Internal Audit
Leadership And Career
On Demand Webinars
Opinion
Resource Library
Risk
Uncategorized
Videos
Webinars
Whitepapers