A|S|A|P®
The Association of Strategic Alliance Professionals

Strategic Alliance QUARTERLY

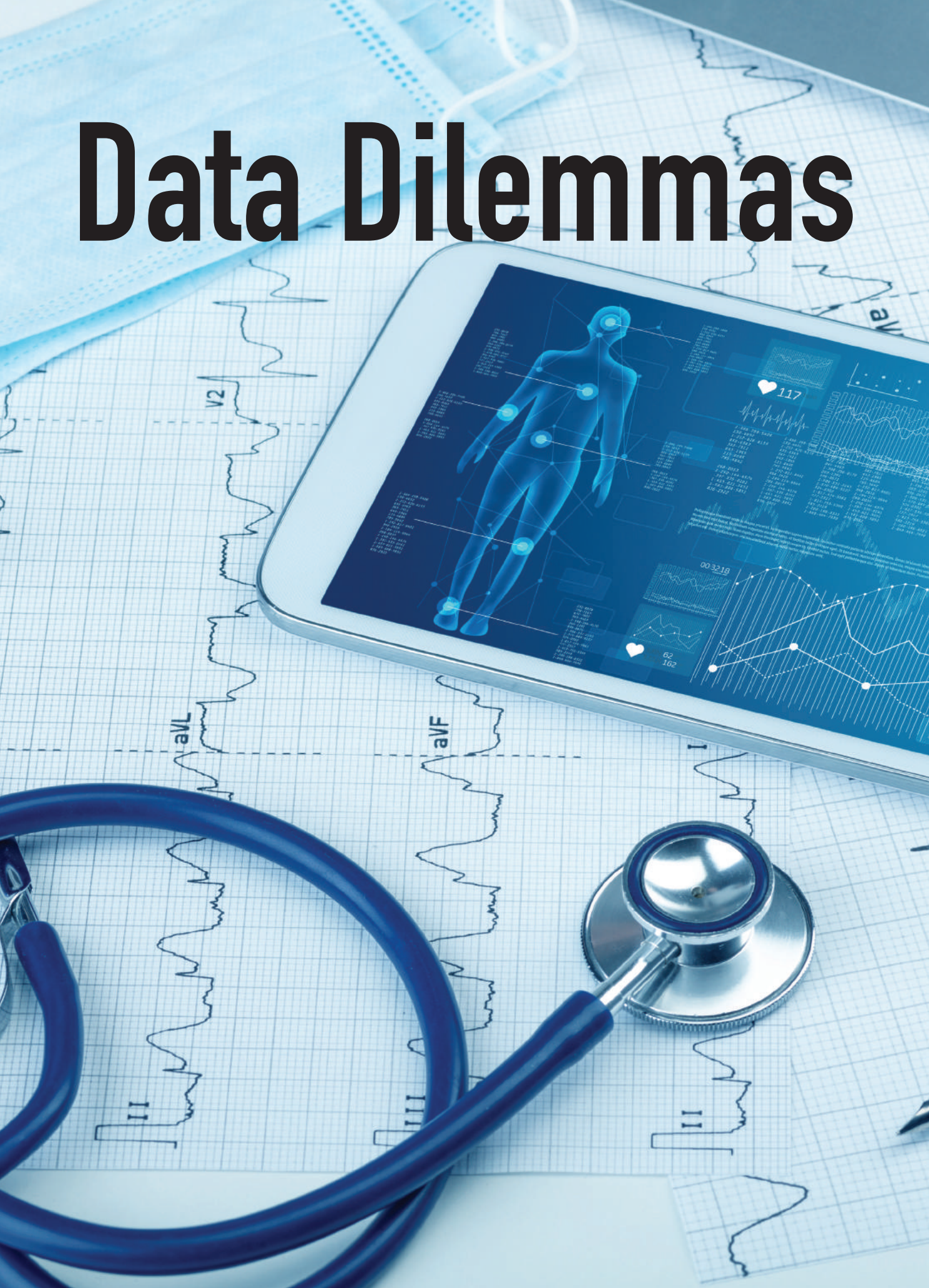
Q2 2020

Partnering in a Pandemic

Alliance Professionals Across Industries and Around the World Share How They've Been Coping with COVID-19

- **Going to Commercial**
  Congratulations! Your Drug Product Just Got Approved and You're Ready to Take It to Market. Now the Real Work Begins
- **Don't Kill That Goose!**
  Coopetition Helps Even the Fiercest Competitors Get Along, with Growth for Both
- **A Process, Not an Afterthought**
  Biopharma Alliance Integration After M&A Activity Works Best with Early Alliance Management Involvement
- **Data Dilemmas**
  Alliance Managers in Data Partnerships Wrestle with Issues of Privacy, Security, Legal Risk, and the Dreaded "Mission Creep"
- ***Editorial Supplement:* Beyond COVID-19**
  You Can Help Your Alliances Not Just Survive, but Emerge Even Stronger from This Crisis

Data Dilemmas



Alliance Managers in Data Partnerships Wrestle with Issues Around Privacy, Security, Legal Risk, IP, and "Mission Creep"

By Jon Lavietes

As you discovered in our last issue, artificial intelligence (AI) alliances are proliferating rapidly ("It's the Data—and a Lot More," Q1 2020), and that trend will likely continue as AI is used to track and fight the spread of COVID-19 around the globe. Meanwhile, best practices in how to manage these partnerships are starting to take shape.

At the heart of any AI collaboration is, of course, data. They say "data is the new oil," and indeed, data is needed to fuel the algorithms that power an AI product or service. Data alliances come in many forms, such as the following, to name a representative sample:

- Google working with academic research institutions, life sciences companies, hospitals, and health systems to produce Verily, a well-funded entity of its parent company Alphabet that aims to transition our healthcare system to one oriented around preventative care by regularly examining research and patient-care data to provide a "feedback loop" that can be used to continually refine all aspects of developing, administering, and monitoring therapies.
- The MELLODDY project, a product of the Innovative Medicines Initiative (IMI), an organization born out of a collaboration between the European Union and the European Federation of Pharmaceutical Industries and Associations (EFPIA) that has universities, research centers, pharmaceutical companies, patient organizations, and regulators working together to develop vaccines, medicines, and treatments in areas where there is an unmet medical or social need. MELLODY uses machine learning (ML) to mine drug discovery data from a who's who of pharmaceutical companies.
- Public-private alliances that deliver the smart factory on a 5G wireless network, where data must be procured, handled, and disposed of carefully like any other asset.

In these contexts, data is no different from any other form of IP, and with it come legal obligations that must be adhered to when using it. Risk management is a high-value service performed by all alliance managers, and when data is at the center of a collaboration they serve as a sturdy bridge between core alliance operation teams and their company's legal departments. Company lawyers generally aren't involved in day-to-day affairs, so it is up to alliance professionals to help protect their companies' interests in the negotiation stage and keep their organizations from running afoul of the law for the alliance's duration. Legal statutes around data continue to evolve, particularly where privacy is concerned, so it is critical that the alliance management function keep several principles in mind when finalizing the contract for and executing a data-driven partnership.

If the Shoe Fits: Starting Data Alliances Off on the Right Foot

When multiple parties initially come together, alliance managers have a meaningful role to play in the actual formation of the contract and in ensuring that it puts the partnership on the right track. Alliance managers are well equipped to ask whether the alliance objectives have practical value, and whether the collaboration is properly structured to generate that value. At the broadest level, all stakeholders need to agree on the alliance's existential purpose and how the data is expected to achieve its end goals.

Brian O'Shaughnessy, partner at Dinsmore & Shohl LLP, urged alliance stewards to be "well acquainted with both research and business managers [involved in the initiative]. Alliance managers should ensure that they know what the enterprise is looking for from both a technical and a business standpoint."

"If you're thinking that everything in the agreement is perfectly stated and contemplates every eventuality in the future, that's a rather naïve outlook. No agreement—no matter how well written—is perfect or prescient."

To that end, O'Shaughnessy recommended that alliance managers work with researchers, data scientists, and anyone else charged with turning data into a new product or service to figure out what type of data will be generated and how those data sets will be structured no later than the term sheet stage—again, while confirming that the data and the experimental protocols fit the stated business purpose underlying the partnership.

"If you are generating a whole lot of data through complicated protocols, and you have negotiated hard to get that data, you better make sure that that data is relevant to your own researchers, and is consistent with the business purpose of the enterprise," said O'Shaughnessy.

Once everybody is in agreement on what type of data will be foundational to the partnership, what new data is expected to be generated along the way, and how that data will drive the collaboration to its desired results, the parties must agree on who owns the resultant IP and how that IP will be protected. As part of that process, the alliance members must determine which data sets are the most valuable and sensitive and handle them with due care. For example, provisions will need to be written into the contract to specifically cover how to store, protect, and share information that constitutes valuable trade secrets—the "secret sauce," if you will. O'Shaughnessy recommended bucketing data sets into tiers of sensitivity, with tier-one data requiring robust handling procedures. (More on those measures later.)

Privacy Is Paramount

Depending on the nature of the data and how it is used, privacy concerns could generate more action items in contract negotiations. First, companies must answer one important question: do these data sets constitute personal information? Or, to put it differently, can that data be used to identify a person? For example, weather for a county in and of itself likely won't reveal the identity of any particular individual. Correlate that weather data with an address or even a Google Earth image of a house, however, and it might pinpoint a person or business. If pharmaceutical companies team up with hospitals and healthcare clinics on COVID-19 research, data around gender, hospital, and zip code should by itself be anonymous. However, all parties must consider whether there is potential for that data to be combined with other information that can unlock the identity of patients at any part of the process.

"You have to make sure that sensitive information you share with [partners] is protected internally, and not just turned over to them in a way that it can be shared throughout their company [and] where you lose control of it."

If it is determined that a collaboration involving EU or California residents relies upon personally identifiable information (PII), then the parties are forced "to make a decision about who they are in the transaction under the law," according to **Rita Heimes**, general counsel and privacy officer for the International Association of Privacy Professionals (IAPP). Under the EU's General Data Protection Regulation (GDPR), "controllers" are defined as entities that provide data sets and chart the direction for what is done with them. "Processors"

generally house, organize, and/or manage the data provided by the controller. For instance, an academic research team developing algorithms on IBM's Watson would be a controller, while Big Blue would be classified as a processor, assuming it was just hosting the work on its platform and not jointly selling it or creating a service with the researchers, in which case both entities would be considered controllers.

"If I'm giving you all of this hot data with private information in it, your reassurances about how secure it will be and your limitations on access are going to be more important than ever."

To comply with the California Consumer Protection Act (CCPA), a company with over $25 million in revenue that buys, receives, sells, or shares the personal information of more than 50,000 California consumers, households, or devices, and derives half of those revenues from selling that personal information to others, must be labeled a "business" in the contract. If a company has a contract with a business to process consumer personal information for specific purposes and is forbidden to use that data in ways not specified in the contract, that organization is labeled a "service provider." Entities that collect data directly from consumers—including internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers—are considered "third parties."

Hot Data Requires Cool Handling

This sets up an interesting push-pull between the parties contributing data to dedicated hosts. The former should protect themselves by demanding representations, warranties, indemnifications, and similar language around the data they are sharing, in Heimes's view.

"[If] I'm giving you all of this hot data with private information in it, your reassurances about how secure it will be and your limitations on access are going to be more important than ever. I, having collected the data from the person in the first place, am ultimately responsible to that person. If I pass along that data to you, I'm going to want you to make me whole again should there be a breach on your end and I have to make good on behalf of my data subjects. These things ultimately flow down to the party that collected the data in the first place. It's really their responsibility to conduct transparency properly with the data subject and take care of that data once it's in their possession," explained Heimes. "The way they can transfer liability is through the contract."

In return, the processor or host should limit its liability vis-à-vis the individuals who have granted the controller consent to use their PII.

"If I'm the data host, I'm most concerned with not getting overexposed in terms of my liability to the ultimate data subject. I don't want to be overexposed in a data breach beyond what I can afford to pay. I don't want to be responsible for having breached promises to the data subject that I never had a chance to communicate with in the first place," said Heimes. "If I'm the host, I probably own security. I can't help it, but that's the risk I take by being willing to host the data. However, I shouldn't bear the privacy responsibility if I had no chance to communicate with the data subject, so I'm going to want to push that back to the party contributing the data."

Before You Gather Data, Collect Your Thoughts

Once the project begins, the alliance must thoroughly think through the initial collection of potential PII if the subjects of the data are California or EU residents. The collector must clearly spell out how it is going to use this information and obtain a concrete consent from the subjects. To comply with GDPR, this acknowledgment cannot be obtained by simply having the end user click a checkbox at the end of several paragraphs of legalese, a form of consent that is common to Web browsers in North America. Rather, the language must be clear and simple to an average citizen (i.e., you don't need a lawyer or a law degree to understand what you are agreeing to).

"Alliance managers should ensure that they know what the enterprise is looking for from both a technical and a business standpoint."

This undertaking is probably a little easier when personal contact with the subjects is a natural part of the process—for instance, when interfacing with patients as part of a clinical trial. Tech companies releasing an app to thousands via a public digital marketplace, however, must carefully craft forms that explain in plain English—again, not lawyer-speak—for

what purpose they are collecting data, how specifically they are going to use that information, and to whom, if anyone, they are going to pass that data along in the process at the point of the transaction.

"You'll always have to answer that [question]: What was the transparency to them at the time of the data collection? Is the sharing consistent with what the data subject understood was going to happen with their data?" said Heimes.

If data is passed along to other alliance members, then alliance managers must make sure that each party corresponds with data subjects in the same detail.

Communication and ongoing monitoring of data alliances "is where alliance managers really earn their money."

"I need to push down to each contributor the responsibility that they are transparent with the data subjects at the point of collection, [that] they [gain] the permission or the right to pass that data along for this particular use," said Heimes.

Service providers that end up selling customer data must be careful as many contracts now contain do-not-sell provisions, which could come back to bite them and the data controllers in the partnership.

Get a Room: Locking Data In and Potential Legal Breaches Out

In many cases, particularly those involving partners that engage in some degree of coopetition, unique measures must be taken to transfer and store data when "there's a great deal of sharing of sensitive, proprietary, confidential, and valuable information," said O'Shaughnessy.

Manufacturers that depend on each other's components in assembling an end-product should not share confidential high-value data through conventional means—i.e., via email, or by enabling partners to download diagnostics, schematics, or other large files onto their servers. Instead, the alliance should set up a "data room," a separate information store that is accessible only to stakeholders in the partner organizations that work with the data firsthand. The goal: to prevent top-tier sensitive data from reaching other partners' servers where they are backed up, nearly impossible to dispose of, and potentially vulnerable to a breach that you are in no position to prevent.

"You have to make sure that sensitive information you share with [partners] is protected internally, and that sensitive information is not just turned over to them in a way that it can be shared throughout their company," said O'Shaughnessy. "You want to make sure alliance members can't share it in a manner where you lose control of it."

Watch Out for "Mission Creep"

Alliance managers in long-term engagements—drug development partnerships or 5G network rollouts, for example—must have their radar in tune for what O'Shaughnessy calls "mission creep or mission diversion." Alliance managers need to "make sure that a) the agreement continues to be properly structured and relevant, and b) the information or whatever you're getting out of that alliance still has relevance to what the [data] scientists are actually doing."

Failure to catch "mission creep" can lead to a variety of unpleasant and unanticipated outcomes, ranging from surrender of valuable information to a termination of the agreement and monetary damages.

Although there's a natural evolution in all long-term alliances, too much "drift" can be problematic. Misalignment between objectives and authorized operations can have significant legal consequences, according to O'Shaughnessy. If data is being collected or used in a manner not authorized in the original agreement, then one party may be unwittingly in breach, despite the best of intentions. Scientists often find that answers to their initial questions reveal new riddles that take them down unanticipated paths. Sometimes this requires collecting new data or using existing data sets in a manner not permitted by the agreement. For example, research teams might want to investigate whether a drug candidate could impact a different disease from the one they initially set out to study, only to find that the contract narrowly limits activities to those that pertain to the original malady. Or, R&D executives may find that data used in animal testing could have some bearing on people not realizing that the agreement prohibits use of that data in relation to research on humans.

Failure to catch this "mission creep" can lead to a variety of unpleasant and unanticipated outcomes, ranging from surrender of valuable information to a termination of the agreement and monetary damages.

"Assuming a healthy and productive relationship can be maintained, it will likely require amendment of the agreement. Such mission creep can best be avoided through routine and candid communication, and mutual reassessment of purpose and protocols," said O'Shaughnessy.

They Work Hard for the Money: Alliance Management and the Contract

In fact, this facilitation of communication and ongoing monitoring of the alliance "is where alliance managers really earn their money," in O'Shaughnessy's mind. "By and large, we all tend to put our blinders on and do what we think needs to be done on a day-to-day basis. Alliances of this nature endure, and they tend to take on a life of their own. Routine communication and a continual reevaluation of purpose ensure that the alliance remains healthy, mutually beneficial, and relevant to the partners' business interests."

If the alliance manager has fostered amicable relations and periodic reexamination of goals throughout the life of an alliance, initiating contract-amendment discussions should be relatively easy if a new direction is needed, an inevitability in many longer-term partnerships which shift over time by nature.

"If you're thinking that everything in the agreement is perfectly stated and contemplates every eventuality in the future, that's a rather naïve outlook," said O'Shaughnessy. "No agreement—no matter how well written—is perfect or prescient."

O'Shaughnessy continued, "In any contract negotiation, it's a good idea to focus on process during the negotiation. This streamlines negotiation, and expedites contract formation. In a long-term agreement, it's important that the agreement itself contemplate a process for downstream amendments. This does two things: 1) it establishes an agreed-upon process for course corrections, and 2) the parties expressly acknowledge that such course corrections are likely to occur during implementation of the contract."

Lofty Standards: Clearing the Bar of Privacy Law by a Healthy Margin

From a privacy perspective, alliance members should also pay attention to standards and ethics practices that are common in their respective industries, beyond following the letter of GDPR, CCPA, and similar regulations that may come to being in the future. The Organization for Economic Cooperation and Development's (OECD) Fair Information Practice Principles provide more assiduous guidance around protecting individuals' private data than any piece of legislation. Privacy by Design, a set of principles popularized by former Ontario information and privacy commissioner Ann Cavoukian a decade ago, can be found with a simple web search. The International Organization for Standardization (ISO) and the National Institute of

Standards and Technology (NIST) continually update privacy recommendations as well.

"Privacy principles that are incorporated into [these] standards are typically more lofty than what the law requires," said Heimes. "By its nature, these laws are written to be generic and not technically specific." By way of example, Heimes noted that privacy legislation generally doesn't specify what level of encryption meets the definition of "reasonable security."

"We all tend to put our blinders on and do what we think needs to be done on a day-to-day basis. Alliances of this nature endure, and they tend to take on a life of their own."

Failure to exceed the letter of the law may leave a collaboration exposed to other blind spots left by the legislation. Heimes cited a hypothetical example of inherent bias in data. Depending on the nature of the activities being conducted, ethics guidelines may require data sets to represent a cross-section of age, ethnicity, income levels, geographies, or other demographics.

Indecent Disposal: Failure to Discard or De-identify Data Results in Legal Risk

Bringing a data-related alliance to an end can be trickier than with the average partnership. O'Shaughnessy noted that agreements often mandate that all parties discard any assets or information exchanged by the parties in a joint initiative. Disposing of a separate data warehouse is much easier than rooting out every email, file, or electronic document relating to intellectual property from an organization's server; actually, the latter is pretty much impossible for an alliance spanning the course of several years.

Privacy regulations are forcing organizations to have a process in place for deleting personal data well before the conclusion of a partner initiative—GDPR grants EU citizens the "right to be forgotten," or the ability to demand that companies remove all PII pertaining to them from their systems. Thus, all alliances should have recurring deletion schedules and a plan in place for excising personal information at the end of the collaboration, including all personal data that got passed to third parties. Full data removal may not be necessary if it is possible to de-identify existing data sets. However, there is currently no way to fully guarantee against hackers

circumnavigating anonymization measures—Heimes has heard of cases of social scientists illustrating the complexity of this task by reidentifying subjects even after HIPAA's guidelines for de-identifying data were followed.

Either way, partners still have to roll up their sleeves and do their best to rid themselves of personal data that is no longer needed for the alliance's purposes.

"It's the hardest part of the job: the follow-up," said Heimes, before anointing anonymizing and deletion schedules as "absolutely the most important security measure in my mind, next to access controls and using good cloud storage."

Legal and privacy concerns might add complications to data alliances, but it is a small price to pay considering the importance of these engagements in fueling several broad trends that are upending the global business landscape: notably AI, ML, the Internet of Things (IoT), and digital transformations.

It's the price of progress. Nothing personal. ■