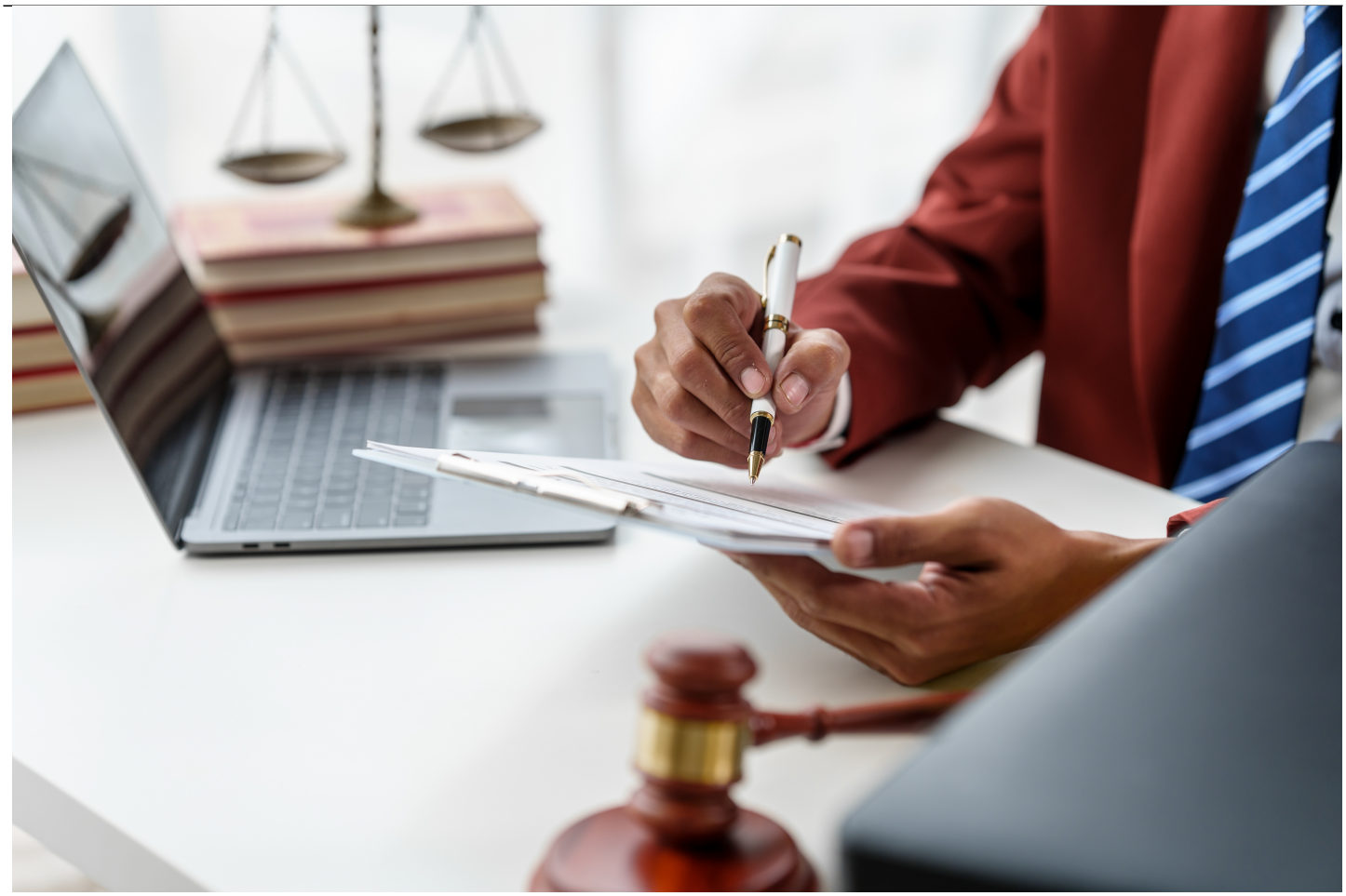
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Paper Protection: How Contracts Secure — and Don’t Secure — Data

Commercial and Contracts

Information Governance

Technology, Privacy, and eCommerce



Banner artwork by NTshutterth / *Shutterstock.com*

Cheat Sheet

- **Data dangers.** Nearly a third of data breaches in 2023 stemmed from third-party data processors, yet sharing digital data with such platforms and business partners is unavoidable.

- **Data processing agreements.** One vehicle for safeguarding data is the DPA, a contractual agreement that defines the respective responsibilities of the “controller” of the data and any “processor” handling personal data on the controller’s behalf.

- **Information security addenda.** DPA’s contractual cousin, the ISA, outlines additional information security standards and requirements. But ISAs are not a legal must, and vary from company to company.

- **Counsel’s role.** In-house counsel should take an active role in guiding the development of such contractual agreements to avoid risk and streamline deal-making with nonlawyer teams.

When it comes to data dangers, headline-grabbing examples are easy to find. A few months ago, Fidelity Investments Life Insurance disclosed that a third-party breach had exposed the personal and financial information of almost 30,000 individuals. That same month, Bank of America reported a similar incident compromising twice as many persons' sensitive data. Both breaches allegedly involved the same third party. In fact, a recent SecurityScorecard report estimates that in 2023 nearly a third of data breaches stemmed from third-party data processors.

Yet to do business in today's interconnected, tech-dependent economy, sharing digital data with third parties — software platforms, business partners, payment processors, and others — is unavoidable. And to protect that data, companies and their in-house counsel routinely turn to, and in some cases legally must turn to, that millennia-old creature of the law: the contract.

The contract provides an endlessly customizable mechanism for spelling out parties' responsibilities and allocating risks. But when it comes to protecting sensitive information, the contract can be a clunky and ineffective tool.

To understand why, one needs to be familiar with two of the most common agreements for safeguarding data: the data processing agreement and information security addendum.

Data processing agreement

For many in-house lawyers, privacy law became mainstream in 2018, when the General Data Protection Regulation (GDPR) took effect in the European Union (EU). Although the privacy law governs the use of EU citizens' personal data, in practice the law reaches across the globe: As a commercial and technological matter, no major international company today can avoid touching GDPR-governed data.

While the GDPR is public law, its governance regime also relies on private contracts. The law requires that a "controller" of personal data enter into a written contract with any "processor" processing personal data on the controller's behalf — a data processing agreement, or DPA.

In the six years since the GDPR's debut, DPAs and similar agreements have become standard features of commercial deals. Some state laws — like the Virginia Consumer Data Protection Act (VCDPA) — similarly require contractual terms on processing personal data (or personal information, as some laws call it). And even where not statutorily mandated, businesses often insist on DPAs as a best practice. Parties benefit from laying out in writing their respective responsibilities over the strictly regulated, high-risk business practice of sharing personal data.

Information security addendum

The DPA has a contractual cousin: an addendum, schedule, or exhibit requiring the data processor to maintain certain information security standards. While there's no uniform name for the document, for consistency this article calls it an information security addendum, or ISA.

Unlike a DPA, the ISA generally isn't a legal must. So while the DPA tends to follow a standard formula — indeed, the GDPR mandates that the DPA address certain issues — the ISA's contents vary from industry to industry and company to company.

The ISA usually imposes more specific and concrete security requirements than the DPA. DPAs tend to eschew granular security specifications in favor of a high-level directive. The GDPR, for instance, demands only that controllers and processors of personal data implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk." And outside certain highly related sectors, federal and state privacy laws in the United States generally also stick to broad standards. (The Health Insurance Portability and Accountability Act — HIPAA, for short — is one exception.)

> Unlike a DPA, the ISA generally isn't a legal must. While the DPA tends to follow a standard formula, the ISA's contents vary from industry to industry and company to company.

An ISA, in contrast, may dictate minimum encryption standards for data transfers or stipulate how frequently a processor must conduct penetration tests. It may also lay out detailed rights and responsibilities for monitoring, auditing, and remedying data security incidents.

It shouldn't be a surprise that businesses rely on private agreements to impose security rules stricter and more detailed than needed under law. Despite the proliferation of privacy statutes and regulations, third-party systems remain among the most vulnerable entry points for cyberattacks. And in-house attorneys, already responsible for DPAs, may intuitively see contracts as the logical way to strengthen and customize their data processors' information security standards.

But if the ISA brings benefits, it also raises concerns.

ISAs aren't typically handled by lawyers

The ISA imposes information security requirements through the legal vehicle of the contract. But the substance of those contractual terms is highly technical and nonlegal.

And while many in-house lawyers today know enough privacy law to negotiate a DPA, ISAs routinely demand tech knowledge beyond that of most members of the legal bar. Even if lawyers follow the jargon — AES-256, NIST, OWASP, and other terms — they may lack insight into their company's IT systems and information security practices to draw up or evaluate ISA requirements.

Commonly then, IT or information security (InfoSec) personnel initially draft — and, on the other side, review — information security addenda.

Business transactions routinely rely on information from nonlawyers, and sometimes laypersons even lead contracting. An acquisition agreement, for instance, contains numerous details provided by financial professionals. In talent deals, agents or managers often draw up deal terms.

But for many organizations, delegating contracting to an IT/InfoSec department can create operational challenges and inefficiencies.

Do's and don'ts for deploying DPAs and ISAs

DON'T: Tack on DPAs and IPAs to every contract, no matter the deal.

DO: Use DPAs and ISAs when the deal requires or warrants it.

DON'T: Assume that the stricter your infosec demands the better.

DO: Tailor your infosec requirements to industry norms, your company's needs, and the deal.

DON'T: Leave information security requirements to IT.

DO: Treat an information security addendum like the contract it is; understand its terms and how they tie into the rest of the contract.

DON'T: Rely solely on contracts to protect your data.

DO: Use both contractual and non-contractual means to keep your data safe (e.g., third-party risk management, audits, certifications).

Unlike finance professionals in M&A transactions or agents and managers in talent deals, the IT/InfoSec personnel setting security requirements will often have little experience in negotiating deals. Yet understanding the soft science of deal-making — its compromises, trade-offs, and pragmatism — is critical for contract writing. That understanding helps drafters appreciate the importance of taking reasonable, market-tested positions and of aligning their contract terms with actual business needs. An unnecessarily aggressive contract stance does little more than generate negotiating friction and lengthen time to deal close.

Without deal-making experience, an IT/InfoSec team may instinctively draft the ISA as a "wishlist" of security demands that are far stricter than their business requires. Indeed, they may think that approach prudent, because a single template can then be used to cover various data processing scenarios, from incidentally seeing business contact details to safeguarding sensitive payment card information.

But the more detailed and demanding the ISA template, the more likely that the IT/InfoSec team on the reviewing end will edit it to fit their own practices or to match market norms. And those mark-ups will in turn require feedback from the drafting party. If the drafting party was seeking more protections than it really needed, a Procrustean template can turn contract review into an exercise in trading redlines.

> If the drafting party was seeking more protections than it really needed, a Procrustean template can turn contract review into an exercise in trading redlines.

Delays can also ensue, as contracting is rarely the IT/InfoSec team's main job. When allocating limited time and resources, they may deprioritize document-editing.

A lack of familiarity with the underlying deal may also lead to drafting conflicts between the ISA and the primary agreement. For instance, for many commercial transactions it's common for "Confidential Information" to carry a defined meaning under both the ISA and the master contract.

But unless the IT/InfoSec team understands the master contract definition — or unless the deal lawyer oversees their editing — contractual ambiguities and inconsistencies can arise.

The result is often an unnecessarily slow and bureaucratic contracting process. But at least it results in more protection, right?

“Words, words, mere words”

Despite these issues, in-house attorneys may still see an ISA as reducing risk on balance. Certainly it makes for a bigger contract: Together with the DPA, these two documents can sometimes exceed the size of the master agreement.

But contracts consist of only words, even if legally enforceable ones. What parties represent through those words may prove untrue or incorrect. Parties sometimes breach contractual obligations.

So too with ISAs. Whatever a data processor promises about its security posture in the contract may not track reality.

And if the data provider refuses to entertain variations to its terms, it may actually widen the gap between contract and fact. Most organizations’ policies and practices won’t perfectly sync with those in a one-size-fits-all template. When a processor signs an ISA without any negotiation, that may actually signal noncompliance. The processor may have failed to read the terms closely — or misrepresented their security state to swiftly close a deal.

In those cases a data provider’s main remedy is a breach of contract claim. But given the practical challenges of detecting a breach; the time, expense and unpredictability of litigation; and the limits of judicial remedies to right wrongs, those remedies are never a business’s first choice. With information security issues, businesses would prefer no breach at all.

> Contracts consist of only words, even if legally enforceable ones. What parties represent through those words may prove untrue or incorrect. Parties sometimes breach contractual obligations.

Keeping data secure while using contracts when needed

Of course, a gap between promise and practice can exist in any contract, not just information addenda.

That isn’t necessarily bad. Imagine the time, effort, and costs if parties insisted on verifying all contractual representations first-hand. It’s cheaper and easier to rely on promises enforceable by a court or arbitrator.

Still, contracts have significant limitations in securing data. And “protection by pagecount” can create inefficiencies and risks.

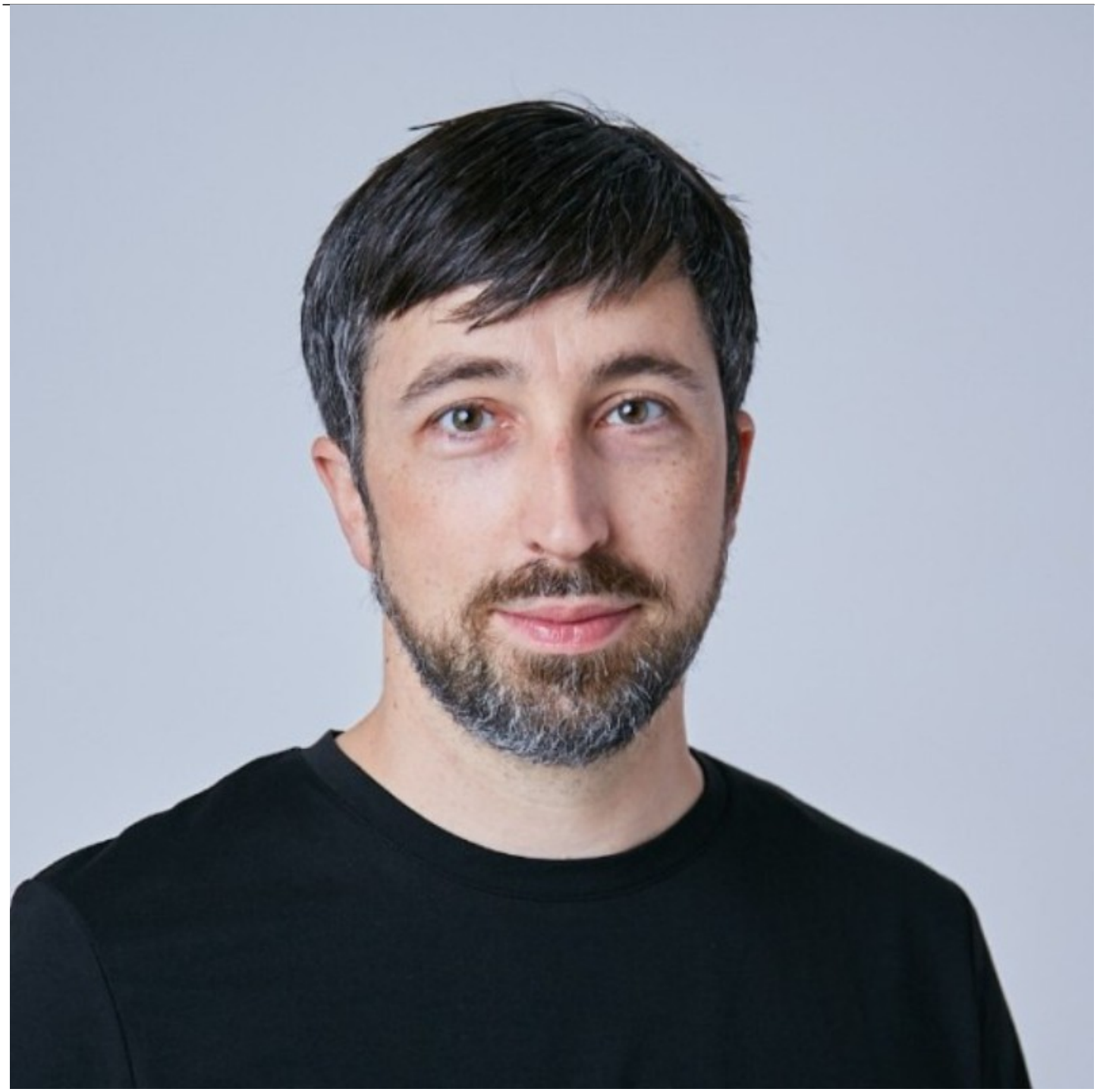
> Contracts have significant limitations in securing data. And “protection by pagecount” can create inefficiencies and risks.

The good news is that business can look to many noncontractual mechanisms to help ensure that third parties safeguard their data. Among the most common means are conducting third-party risk management, seeking third-party cybersecurity certifications like SOC2 and ISO 27001, which allow businesses to avoid relying on bare representations from their counterparty. Organizations might also conduct information security audits on their processors. In addition, businesses should obtain proof of cyberinsurance; without that, many data processors will lack the financial resources to address and remedy a security breach.

With or without a standalone ISA, contracts still play a critical role in cybersecurity. DPAs are often legally required, and in-house lawyers can incorporate information security warranties into any contract, along with audit rights and an indemnity for data breaches. In some cases — particularly when large amounts of data or highly sensitive information is at issue — comprehensive ISAs are the best approach.

But in many commercial transactions, extensive information security contracts create little more than deal delays, while providing only paper protection.

Christopher Wlach



General Counsel

Huge

Chris Wlach is the general counsel of Huge, a creative consultancy owned by the Interpublic Group of Companies, Inc. Before moving in-house he focused on complex commercial litigation at Arnold & Porter. He is a Certified Information Privacy Professional (CIPP/US) through the International Association of Privacy Professionals. He also chairs the board of HEART, a humane education nonprofit.