INSIGHTS

Due Diligence Insights | FALL 2026

iab. LEGAL AFFAIRS & PUBLIC POLICY

# Vendor Diligence Obligations After Delaware HB 380

## Introduction



In 2018, GDPR established that a data controller must ensure the lawful processing of the personal data it collects, including processing performed by vendors (processors) on the controller's behalf[1].

The principle that a data controller is responsible for ensuring that its vendors lawfully process its personal data is also enshrined in U.S. state privacy laws. According to the Minnesota Attorney General, remarking about controller responsibilities under the Minnesota Consumer Data Privacy Act:

> *[T]he Act holds that a controller is responsible for all of the duties and responsibilities imposed on a controller even where a controller has deferred control of data to a third-party processor. (emphasis added)*

Marketplaces and Insight Platforms support the use of data and derived insights across participants in the advertising ecosystem. Their architecture and operating models vary, but they share an objective: enabling organizations to work

> *To the extent it has not already done so, FedEx shall develop and maintain a process for the onboarding of third parties with whom FedEx directly sells or shares personal information. (emphasis added)*

What is this onboarding process? More generally, what are a controller's obligations to conduct diligence on vendors and third-parties? Do these obligations differ depending on the vendor's processing role, whether processor or third-party, or perhaps on the sensitivity of the personal data being processed?

This article explores the reasons and requirements for privacy due diligence, especially for the digital advertising industry. It begins with a brief overview of the principles behind the diligence obligations in the privacy laws (the "whys"). It then outlines the specific requirements for diligence (the "whats"), including how Delaware House Bill 380 (DE HB380) substantially raises the bar for required diligence. It concludes with a discussion of the implications of the diligence requirements for the digital advertising industry, including possible solutions for performing diligence efficiently and at scale.

## Part 1: Overview of Due Diligence Principles

Where does the idea originate that a controller is responsible for its vendors' processing of controller personal data? In 1973 (over 50 years ago), the US Department of Health, Education and Welfare (HEW) formed an advisory committee to report on the potentially adverse effects of "using computers to keep records about people[2]." This report became the basis for the Organisation for Economic Co-operation and Development's Fair Information Practice Principles (FIPPS), which in turn are the basis for most modern privacy laws.

The HEW report's first recommendation was to prohibit personal data transfers without consent to an organization that was not subject to the committee's proposed "safeguard requirements." Privacy diligence was born.

More recently, GDPR established three key concepts for processor governance by controllers:

**1 – Binding Contracts with processors:**
Art 28(3): Processing by a processor shall be governed by a contract that complies with a specified list of requirements.

**2 – Due Diligence on processors:**
GDPR Art 28 addresses both sides of the diligence requirement. Under GDPR Art 28(1), the controller may use only processors providing sufficient guarantees that the processing will meet the requirements of GDPR. Under GDPR Art 28(3)(f), the processor must assist the controller in ensuring compliance with the controller's obligations in Articles 32 through 36. Worth noting is that this assistance obligation includes GDPR Article 35, which sets out the requirements for data protection impact assessments, or DPIAs. This means processors must assist controllers with completing DPIAs that relate to the processors' processing activities.

**3 – Subprocessor authorization and flow-down obligations**
Art 28(2) requires controller approval for the use of subprocessors, and Art 28(4) requires contracts between processors and their subprocessors.

All of the U.S. state privacy laws adopt these key concepts in some form. In the California and Delaware laws, they have been further developed into specific, prescriptive requirements.

All of the U.S. state privacy laws adopt these key concepts in some form. In the California and Delaware laws, they have been further developed into specific, prescriptive requirements.

## Part 2: Due Diligence Requirements and Delaware HB380

Part 2 of this document explores why vendor due diligence is an increasing focus of legislators and privacy regulators, the role of contracts in vendor diligence, and how DE HB380, which amends Delaware's existing omnibus privacy law, increases the minimum requirements for vendor due diligence.

**The Increasing Regulatory Focus on Privacy Due Diligence**

To answer why we are seeing an increased regulatory focus on vendor privacy diligence, it is worth looking back. First, legal and regulatory scrutiny tends to increase when a product or service becomes viewed as potentially harmful to people without regulation, such as in the prescription drugs market. Where the harms to people arise as much from data uses in ecosystems as from discrete uses by individual companies, regulatory scrutiny of not only the individual actors that comprise the ecosystem, but also the data flows among them, is not surprising.

In privacy terms, the personal data processing ecosystem consists of personal data flowing from consumers to controllers, and then from controllers to their processors and third parties. Mandatory contracts and vendor diligence are the primary methods for asserting regulatory oversight of these ecosystem data flows. In addition to mandatory privacy contract terms, we see recent evidence of this ecosystem focus in the CCPA risk assessment regulations, which require evaluating the processors and third-parties that are involved in the activity being assessed, and in the new mandatory diligence obligations from DE HB380.

In large organizations, vendor diligence often lives in one or more procurement departments that for decades have employed requests for information (RFIs) as the primary approach for conducting vendor diligence. RFIs work well when they are standardized, such as Information Security assessments that are standardized around the SOC2 and ISO 27001 frameworks. Similar standardization of privacy compliance principles is emerging but remains challenging, especially in the United States due to the prolifieration of similar but not identical state privacy laws.

The current state of play for questionnaires in privacy diligence is to use RFI's to assess vendor compliance and risk; however, absent industry standards for conducting privacy diligence like those used in the information security domain, companies have necessarily created their own, bespoke privacy RFIs, which are often appended to information security questionnaires. The lack of standardization among privacy RFIs has efficiency costs, however, as discussed further below.

**The Role of Contracts in Vendor Due Diligence**

The requirements for contracts between controllers and their processors and third-parties is not the primary focus of this piece, but as they relate to controllers' due diligence obligations, the following points are worth noting:

- **Processing is prohibited without compliant contracts.** Not only are contracts required by law, but processors and third-parties are flatly prohibited from processing the controller's personal data without a contract. (See CCPA Regulations Sections 7050(e) and 7052(a); Delaware HB380 §12D-107A(a))

- **Contracts require processors to cooperate with controllers' efforts to comply with privacy laws.** Controller-to-processor contracts must include statutorily mandated language giving the controller the right to ensure the processor is complying with both the contract and the relevant law (see, e.g., CCPA Reg. 7051(a)(6); DE HB380 §12D-107(b)(3)). Under DE HB380, the processor contracts must require processors to make available to the controller all information in its possession necessary to demonstrate the processor's compliance with HB380 and cooperate with reasonable assessments by the controller or the controller's designated assessor in order to conduct due diligence.
- **Third-party contracts require participation in controllers' due diligence questionnaires and document reviews.** Controller-to-third-party contracts go even further, and DE HB380 now sets the high bar requirement. Under DE HB380 §12D-106(10)(c), third-party contracts must grant the controller rights to take reasonable and appropriate steps to ensure that the third party uses the personal data transferred by the controller in a manner consistent with the controller's obligations under HB380, which include the new, mandatory due diligence requirements discussed below.

The controllers' duty to have contracts with their processors and third-parties is not only required by law, but also under DE HB380 the contract terms must require third-parties to participate in HB380's prescriptive due diligence activities.

**Due Diligence under Delaware HB380**

Delaware HB380 imposes new, specific diligence requirements for how controllers must conduct due diligence on third-parties[3]. The new requirements take effect January 1, 2027, and they raise the compliance bar considerably. Under DE HB380 §12D-106(11), a controller shall:

> *Conduct reasonable due diligence, either by the controller or through a designated assessor, of third parties to whom the controller discloses personal data, including the sale of personal data and targeted advertising ….*
>
> *Reasonable due diligence involves, at a minimum, assessing the third party through the use of questionnaires and review of relevant documents of the third party.*
>
> *Additional reasonable measures must be undertaken in a manner that is commensurate with the sensitivity of the data disclosed by the controller to the processor or third party.*

There are three key takeaways from the statute:

1. Conducting in-depth diligence of third-parties is mandatory.
2. Third-party diligence now has a minimum, defined floor: controllers must use questionnaires to assess their third-parties and also review relevant third-party documentation.
3. In addition to the minimum assessment activities, controllers must employ supplemental measures depending on the sensitivity of the data disclosed by the controller. Notably, this duty applies to the controller's assessments of processors as well.

**Meeting the Floor: What are Questionnaires and Relevant Documents?**

Delaware HB380 clearly states that the minimum diligence required to assess third-parties must include the use of questionnaires and reviews of relevant documents. A natural follow-on question is, "Which questionnaires and documents?"

Clearly, a well-drafted privacy RFI is a type of questionnaire that will suffice to meet DE HB380's requirements. However, the controllers' challenge in a world of heterogenous privacy laws is to create privacy RFIs that are accurate and comprehensive enough, and sufficiently tuned to the sensitivity of the personal data that the vendor will process, to elicit the vendor information needed to properly assess the risks created by the vendor's processing. This is no small challenge in an environment of rapidly evolving privacy laws.

Deciding which vendor documents are relevant for properly assessing privacy risks is often a contextual exercise, again because the nature of the vendor's processing and the sensitivity of the personal data being processed can vary widely.

We can, however, point to several foundational documents that should be included in vendor diligence assessments:

- privacy policies
- information security measures
- lists of sub-processors and their processing details
- descriptions of both the vendor's processing methods and the nature of the personal data being processed
- data flows and maps are also highly contextual, but they are also extremely important when assessing vendor risk.



## Part 3: Diligence for the Digital Advertising Industry

As noted, one reason for increased regulatory focus on vendor diligence is the risks associated with the transmission of personal data throughout the internet and digital ecosystems. The digital advertising industry is one of the largest digital ecosystems, and it is no secret that U.S. privacy laws are particularly focused on regulating personal data used for targeted advertising. Ongoing regulatory attention on digital advertising is a likely consequence of these facts. Delaware HB380 is a sign that this attention is increasingly focused on the relationships among ecosystem participants, and not only on the participants themselves.

**First Parties (Publishers/Advertisers) on the Front Lines**

First parties – primarily publishers and advertisers in the digital advertising ecosystem – are the controllers that have the most urgent need to address vendor privacy diligence. They are the industry's controllers, because they have the primary relationship with the consumers that buy their products, visit their websites, and use their apps. DE HB380 clearly puts the primary diligence obligation on them.

**Ad Tech Intermediaries Accepting (demanding?) Controller Rights**

However, increasingly advertising technology (ad tech) intermediaries are controllers too, for two reasons. One is that CCPA Reg. 7050(b) specifically says that a company that contracts with a controller to provide targeted advertising is a third-party, not a processor (the regulation uses CCPA's terminology, of course). The second reason is that ad tech intermediaries – perhaps feeling compelled by Reg 7050(b) to do so – increasingly negotiate for independent controller rights in their contracts with publishers and advertisers. Whenever they are controllers, the DE HB380's heightened diligence requirements apply to ad tech intermediaries as well.

**Governance Trends in Digital Advertising: How the IAB Can Help the Digital Advertising Industry with Vendor Diligence Obligations**

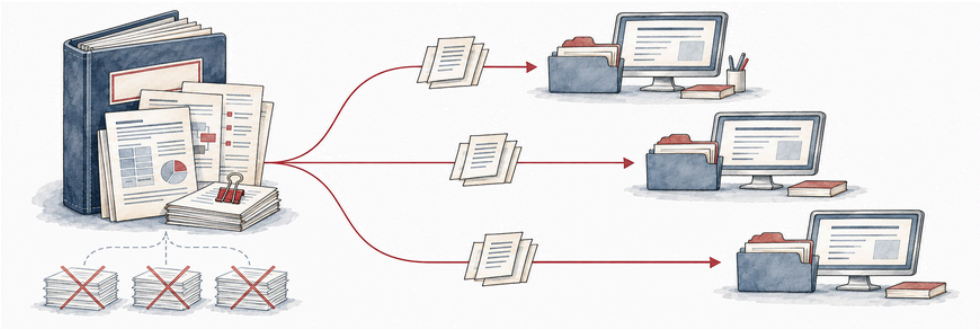
For years now, the IAB has helped industry participants understand the privacy law compliance challenges for the digital advertising industry[4,5,6]. One of the key challenges is establishing controller-to-processor/third party contracts in the RTB environment, where personal data can be shared with many participants, starting with the data in publishers' bid requests flowing to SSPs and DSPs, followed by personal data gathered by DSPs to enhance advertisers' media planning, buying and targeting precision, and ending with measurement providers collecting data from publishers and advertisers to report on reach and attribution.

The number of touchpoints in a single RTB transaction can make establishing the statutorily-mandated contract terms among the various controllers, processors, and third-parties a daunting task. Addressing this challenge is the purpose of the IAB's Multi-State Privacy Agreement (MSPA), a standardized contractual framework that works hand in glove with the Global Privacy Platform (GPP) to ensure MSPA participants can put the right contractual terms in place with other

participants after receiving the consumer signals delivered via the GPP. The MSPA is a tool to enable ecosystem-wide privacy compliance among participants who may not even know each other, much less have the required contract terms in place.

Similarly, to help participants in the digital advertising industry conduct vendor privacy diligence, the IAB introduced the IAB Diligence Platform powered by SafeGuard Privacy[7]. The IAB Diligence Platform combines privacy law compliance assessments with relationship-specific data flow questionnaires. For example, the IAB questionnaires include modules for Publisher-to-SSP and Advertiser/Agency-to-DSP data flows. The questionnaires also help surface the specific privacy compliance obligations that result from these relationships and their data uses.

Using the IAB Diligence Platform, vendors can complete these standardized assessments and questionnaires once and then easily and securely share them with multiple controllers when requested. Similarly, the vendors can share relevant supporting documentation with their controllers. The IAB Diligence Platform's standardized approach to vendor diligence is an important tool and enabler for controllers that need to meet their DE HB380 third party diligence obligations. These tools and capabilities apply equally well for processor diligence assessments.



## Part 4: Summary and Practical Recommendations

**Summary**

Part 1 of this article showed that the origins of privacy due diligence began as early as the 1970s, when the OECD released the Fair Information Practice Principles. It showed that, more recently, GDPR imposed mandatory vendor diligence through the principle that controllers are liable for the use of personal data their behalfs, even when the processing is performed by processors.

Part 2 explored why legislators and privacy regulators are increasing their focuse on vendor due diligence, the importance of contracts to vendor diligence programs, and how Delaware HB380 increases the minimum requirements for vendor due diligence.

Part 3 illustrated the effects of mandatory diligence obligations on the digital advertising industry, especially on first parties, like publishers and advertisers. It explored the challenges that the digital advertising ecosystem presents for effective vendor diligence, along with the IAB's efforts to standardize privacy contracts and diligence for the industry through the MSPA and the IAB Diligence Platform.

**Recommendations**

Global privacy laws impose two, primary requirements on controllers regarding the processors and third-parties that use the controllers' personal data. These obligations must be fulfilled before to the vendors' and third-parties' processing begins.

**Contracts**

- Execute contracts with processors and third-parties that meet the specific requirements set forth in the laws. One of these requirements is language requiring cooperation with the controllers' due diligence efforts. Where the contract is with a third-party, it should require completing the controller's questionnaires and providing reasonable supporting documentation for the controller's review.

**Minimum Diligence Activities and Timing:**

- DE HB380 sets the minimum floor for third-party diligence, and arguably for processor diligence where sensitive data are involved. The law requires diligence to include the use of questionnaires and relevant document reviews. Additional diligence may be required if the processing involves sensitive personal data.
- The CCPA risk assessment regulations require that where risk assessments are mandatory, such as for cross-context behavioral advertising purposes (which typically involve processing by service providers, third-parties, or both), the risk assessment must be completed prior to commencing the processing.

**Consider IAB Contract and Diligence Offerings**

- In the digital advertising industry, controllers should consider using the IAB's offerings for contracts (the Multi-State Privacy Agreement) and diligence (the IAB Diligence Platform), which are specifically designed to increase efficiencies and improve compliance for the digital advertising industry as a whole.

## Notes:

[1]For purposes of this article, unless the context requires otherwise, the term "controller" includes "business," and "processor" includes both "service provider" and "third party," as those terms are defined in the California Consumer Privacy Act (CCPA).

[2]Secretary's Advisory Committee on Automated Personal Data Systems. (1973, July). Records, computers and the rights of citizens. U.S. Department of Health, Education, and Welfare. https://archive.epic.org/privacy/hew1973report/. archive.epic.org

[3]Delaware Personal Data Privacy Act, Del. Code Ann. tit. 6, § 12D-102(37) (2026) (effective January 1, 2027). "Third party" means, with respect to personal data controlled by a controller, any person other than the relevant consumer, the controller of such personal data, or a processor or an affiliate of the processor or the controller, except for entities listed under § 12D-103(b) of this title. https://delcode.delaware.gov/title6/c012D/index.html. delcode.delaware.gov

[4]Hahn, M., & Glassberg, R. (2026, March 26). 2026 IAB Diligence Platform expansion: A conversation with industry leaders. Interactive Advertising Bureau. https://www.iab.com/blog/iab-diligence-privacy-compliance-expansion/. iab.com

[5]Interactive Advertising Bureau. (2025, April). Data clean rooms: A U.S. state privacy law perspective. *https://www.iab.com/wp-content/uploads/2025/04/IAB_Data_Clean_Rooms_A_US_State_Privacy_Law_Perspective_April-2025.pdf*. iab.com

[6]Hahn, M. (2025, July 11). How a recent settlement represents a warning and relief for the adtech industry. IAPP.

[7]https://iapp.org/news/a/how-a-recent-settlement-represents-a-warning-and-relief-for-the-adtech-industry. IAPP

Author disclosure: The author is the general counsel of SafeGuard Privacy.

## Author



**Andy Hepburn**
General Counsel
Safeguard Privacy