Drowning in DPAs?

Practical Tips for Privacy Agreements in a Shifting Legal Landscape

Leah A. Druckerman, Esq.
Counsel, Technology & Innovation, Venable LLP | ladruckerman@Venable.com

Desarie Green, Esq.
Sr. Privacy Counsel, Cengage Learning, Inc. | desarie.green@cengage.com

VENABLE LLP

Outline

- DPA Basics
- Regulatory Trends
- DPAs in Practice and Key Friction Points
- Liability and Risk Allocations
- Tips and Takeaways

VENABLE LLP

DPA Basics

VENABLE LLP

What Is a DPA?

- Addresses **statutory requirements for a given transaction** or relationship involving personal data
  - Most privacy laws have contracting requirements
    - GDPR Article 28 – Controller-to-processor contract requirements
    - CCPA/CPRA
      - 11 CCR 7051(a) – Business-to-service provider contract requirements
      - 11 CCR 7053(a) – Business-to-third party contract requirements
    - HIPAA – 45 CFR 164.504(e) – Covered entity-to-business associate contract requirements
    - Industry-specific terms – Access4Learning Student Data Privacy Coalition National DPA

- Can include other terms as well
  - Security requirements, risk allocations, creation/use of deidentified data, AI terms

- Today's focus is primarily on controller-to-processor DPAs under omnibus privacy laws

VENABLE LLP

What Goes in a Typical Processor DPA?

- Processing Restrictions
- Compliance with Laws
- Assistance
- Confidentiality
- Subprocessor Management
- Data Security
- Audits
- International Transfers (if applicable)
- Return/Deletion
- Description of Processing

VENABLE LLP

What Goes in a California "Third Party" DPA?

- Processing Restrictions
- Compliance with Laws
- "Audits" (disclosing party has right to take steps to ensure compliance and stop and remediate unauthorized processing)
- Description of Processing

VENABLE LLP

What Challenges Do DPAs Present?

- Context-sensitive and not always possible to create a “one size fits all” document
  - Legal requirements and company risk tolerances vary based on the services, the data involved, the data flows at issue, how and for what purposes the data is being processed, etc.
  - Often requires customization for each engagement (descriptions of processing, etc.)

- DPA terms can have significant operational impacts on signatories
  - Data use/disclosure restrictions
  - Audit rights
  - Subcontracting restrictions
  - Specific security requirements

- DPA risk allocations can be significant and are commonly negotiated
  - Liability caps/waivers
  - Indemnity rights
  - Data breach and compliance assistance cost-shifting

VENABLE LLP

DPA Trends

VENABLE LLP

DPA Regulatory Enforcement

- Contracting has been a focus area for California regulators. Notably, enforcement actions brought this year specifically identify outdated, "boilerplate," or noncompliant DPAs as violations of CCPA
- Some key takeaways:
  - Make sure DPAs, especially for higher-risk processing relationships, are periodically updated and include all required terms
  - DPAs must include specific processing descriptions, with the following being held insufficient:
    - "Any business purpose"
    - "Any internal use inuring to the recipient's direct benefit"
    - "Purposes contemplated in the agreement"
    - "As otherwise specified in writing" with no other written instructions/descriptions
  - CCPA's "safe harbor" that limits a business's liability when it communicates a data subject's opt-out request is contingent on the business not having a "reason to believe" that the recipient will further sell the data
    - Regulators suggest using "clear contractual language" regarding prohibitions on sale of opted-out data

VENABLE LLP

Trends in State Law DPA Requirements

- Colorado-style independent audits (see C.R.S. 6-1-1305(5)(d)(II)(B))
  - Processor can arrange for a "qualified and independent auditor" to conduct an audit or assessment at least annually at the processor's expense, pursuant to an "appropriate and accepted control standard or framework and audit procedure," and provide an audit report to the controller upon request
    - Commonly see SOC 2 Type II, HITRUST, ISO/IEC 27XXX

- Notice and right to object to subprocessors
  - Existing GDPR obligation, now required in Colorado, Maryland, and a growing number of state privacy laws

- More specific obligations regarding data subject rights
  - Example: Maryland's MODPA requires processors to agree to delete personal data upon request

VENABLE LLP

Bulk Data Rule & The Protecting Americans' Data from Foreign Adversaries Act

- U.S. federal laws restricting international data transfers have arrived!

- **BDR's** data transfer restrictions prohibit the transfer of government-related data or "bulk" sensitive data to prohibited persons and entities
  - Applies to deidentified, encrypted, pseudonymized, or aggregated data
  - Contract requirements for "prohibited" and "restricted" transactions involving data brokerage, including reporting obligations if breached
    - Sample contract language provided by DOJ in Section III(B)(1) of its April 11, 2025 DATA SECURITY PROGRAM: COMPLIANCE GUIDE (https://www.justice.gov/opa/media/1396356/dl)

- **PADFAA's** data transfer restrictions apply to data brokerage of personally identifiable sensitive data *regardless of processing volume* to prohibited persons and entities
  - While not expressly required, we have seen an uptick in contract provisions that require that an entity will not share regulated data with a foreign adversary country.

VENABLE LLP

Artificial Intelligence

- Concerns regarding training data
  - Personal data, confidential information, trade secrets, or IP that clients don't want used for training
  - AI training and processing restrictions (and authorizations!) show up in DPAs

- Approaches to AI processing restrictions
  - Customer consent/approval prior to using customer data to train or improve AI tools
    - Can be scoped for GenAI or to apply more broadly
  - Remediation and mitigation requirements for unauthorized AI use
  - Human review for AI-generated code

VENABLE LLP

DPAs in Practice

VENABLE LLP

Goals of DPA Review

1. Comply with laws and legal requirements
2. Protect the organization's personal data
3. Stay within the organization's risk tolerance
4. Ensure that the services and/or personal data can be used for the desired purposes
5. **Do not unduly hold up deal flow/sales process**

VENABLE LLP

DPA Review Goals: How Do We Get There?

- **Comply with laws and legal requirements**
  - Create and regularly update template DPA(s) for common processing scenarios.
  - Create a checklist for reviewing counterparty DPAs.
- **Protect the organization's personal data**
  - Evaluate the risks presented by the processing and tailor risk allocations, processing restrictions, and other requirements accordingly
- **Stay within organization's risk tolerance**
  - Review and negotiate limitations of liability, liability caps, and cost-shifting items; obtain business approval or input where necessary
- **Ensure that the services and/or personal data can be used for the desired purposes**
  - Review processing restrictions against intended use cases
- **Do not unduly hold up deal flow/sales process**
  - Use templates, checklists, and playbooks with approved fallbacks to reduce review time
  - Keep DPA terms reasonable where appropriate
  - Develop and maintain escalation paths with relevant internal resources

VENABLE LLP

Before You Dive In: Understand the Deal

- Understand **the services**
  - Is the organization the service provider or service recipient?
  - How and for what purposes will personal data be used?
  - What risks do the services present to the organization and to the data subjects?
  - Are the services subject to specific requirements (e.g., adtech and CPRA)
- Understand **processing roles**
  - Is the organization a controller or processor?
  - Is the counterparty a processor or controller/third party, or both?
- Understand **data and data flows**
  - Types of data and data subjects
    - Regulated data, “sensitive” data, employee vs. consumer data
  - Third-party recipients and data flows
    - Subprocessors/subcontractors
    - International data transfers

VENABLE LLP

Key Statutory DPA Friction Points

- **Processing Restrictions**
- Compliance with Laws
- **Assistance**
- Confidentiality
- **Subprocessor Management**
- **Data Security**
- **Audits**
- International Transfers (if applicable)
- Return/Deletion
- **Description of Processing**

VENABLE LLP

Processing Restrictions

- Generally, processors are prohibited from processing personal data except as instructed by the controller and/or as necessary to provide the contracted-for services to the controller.

- Common friction points:
  - Processor use of data for training, building, development, or improvement of services and algorithms
  - Processor creation, use, and disclosure of deidentified or aggregated information
  - Processor creation, use, and disclosure of "usage data" or "analytics data" (e.g., user interactions with service, website, content, etc.)
  - "Split" relationships where a party is a processor for one type of service or category of data but a controller for others
  - Limits on controller instructions to the processor
  - Scope of permitted processing for controller recipient's use of personal data

VENABLE LLP

Assistance

- Generally, processors are required to assist the controller with compliance-related activities in several ways, including:
  - Providing assistance in complying with and effectuating data subject requests
  - Assisting with required data protection assessments or consultations
  - Demonstrating compliance with privacy laws
  - Allowing the controller to stop and remediate unauthorized processing

- Common friction points:
  - Cost-shifting for compliance assistance
  - Timelines/deadlines for compliance assistance
  - Scope of provided assistance

VENABLE LLP

Subprocessor Management

- Many privacy laws give the controller some control over the processor's use of its own processors (subprocessors) to process controller data. A growing number of laws (GDPR, CPA, MODPA, others) require that the controller either:
  - Provide prior consent before the processor may engage a subprocessor or
  - Receive prior notice and have an opportunity to object to the engagement of a subprocessor

- Common friction points:
  - Requiring prior consent instead of notice and opportunity to object
  - Amount of prior notice needed
  - Methods of notice (e.g., subprocessor lists)
  - Permitted grounds for subprocessor objections
  - Handling of objections to subprocessor engagements

VENABLE LLP

Data Security – Data Breaches

- Generally, processors are required to:
  - Notify controllers “without undue delay” of any personal data breach and
  - Provide assistance to the controller to allow the controller to meet its obligations to notify data subjects and government regulators of the personal data breach

- Common Friction Points:
  - Unnecessarily short breach notice timelines
  - Extremely broad “personal data breach” definitions
  - Cost-shifting (to be discussed later)
  - Control over notification process

VENABLE LLP

Data Security – Security Measures

- Generally, processors are required to implement "reasonable" or "appropriate" security measures to protect personal data, taking into account the nature and sensitivity of the information, the risks to the data subject, the state of the art, etc.

- Common Friction Points:
  - Unusually specific or restrictive security requirements
  - Requiring the processor to change or implement additional security safeguards at the controller's request and without any sort of compensation or cost-shifting
  - Requiring remediation of "all" vulnerabilities or risks without consideration of severity

- **Tip:** If you want a nice "general" set of information security requirements that most mature organizations should be able to agree to, the requirements imposed by the NYDFS Cybersecurity Regulation (23 NYCRR Part 500) are a useful checklist

VENABLE LLP

Audits

- Generally, processors are required to allow for and contribute to audits by the controller and their designee. Recent U.S. privacy laws allow for the use of independent audits pursuant to an acceptable standard in lieu of a controller audit.

- Common Friction Points:
  - Independent audits vs. controller audits
  - Audit notice/timing
  - Scope of audit
  - Confidentiality for audit findings
  - Remediation of findings
  - Cost-shifting

VENABLE LLP

Description of Processing

- Generally, DPAs must include some amount of information about the proposed processing of personal data, including (without limitation and depending on applicable law):
  - the nature and purpose of the processing
  - the duration of the processing
  - the types of personal data to be processed and
  - the types of data subjects about whom personal data is processed

- Regulators are scrutinizing descriptions of processing in investigations (see *Healthline*) and expect an appropriate level of specificity:
  - "The business purpose(s) shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific." 11 CCR 7051(a)(2)

- Obtaining and properly documenting this information can be challenging and is often overlooked, particularly from a contract administration perspective

VENABLE LLP

Risk and Liability Considerations

VENABLE LLP

Cost-Shifting

- What is cost-shifting?
  - One party will pay or reimburse the other for certain costs as allocated by the contract
  - Commonly arises in connection with data breaches, audit rights, and compliance assistance

- Where it is offered at all, processors often try to limit data breach reimbursement to "legally required" notifications and/or credit monitoring services

- Responsibility triggers for data breaches (in descending order of customer-friendliness):
  - Vendor pays for any security breach
  - Vendor pays for a security breach, except for one caused by customer
  - Vendor pays for security breach to the extent caused by vendor (or vendor's subprocessors)
  - Vendor pays for security breach to the extent caused by vendor's breach of terms of DPA
  - Vendor does not pay for any security breach

VENABLE LLP

Liability Caps

- Uncapped liability for privacy or security violations is a common ask from controllers, while processors are often looking to limit or cap their liability. These terms are heavily negotiated.
  - Use super-caps and exceptions to tailor exposure levels
  - Put together guidance and fallbacks to limit the number of escalations
  - Read in context with the risk allocations in the underlying agreement
- Carefully consider scope of any exceptions/exclusions
  - Breach of confidentiality terms vs. data security breaches vs. breaches of the DPA

- **Note:** Special / incidental damages waivers can waive security breach damages!
  - *Princeton Community Hosp. Assn. v. Nuance Communs., Inc.*, 2020 U.S. Dist. LEXIS 60490 (S.D. W. Va. Apr. 6, 2020 No. 1:19-00265)
  - *Spec's Family Partners Ltd. v. First Data Merch. Serv. Corp.*, 2017 WL 4547168 (W.D. Tenn. Jul. 7, 2017) – affirmed by the 6th Circuit in 2019
  - *Silverpop Sys., Inc. v. Leading Market Technologies, Inc.*, 641 F. App'x 849 (11th Cir. 2016)
  - Common work-around: Exceptions or designating certain breach-related damages as "direct" damages

VENABLE LLP

Indemnification

- What is an indemnity right?
  - One party agrees to defend and hold harmless the other for losses arising out of specified claims or circumstances
- Reviewing indemnity rights:
  - Consider the indemnity right in context. For example:
    - Analyze whether a client is being asked to indemnify for matters that it can control
    - Look at liability caps and waivers to identify whether indemnity rights are capped or uncapped
  - For mutual indemnity rights, analyze whether the indemnity weighs more strongly upon the client or the counterparty
  - The risk and strength of indemnities for breach of a DPA depend on how particular the DPA is with respect to the measures that must be taken
  - Watch for duplicative or overlapping indemnity rights in DPAs and MSAs

VENABLE LLP

Insurance Coverage

- Downward trend in insurance covering privacy and data breach scenarios
  - Narrowing coverage
  - Increased cost of coverage

- Brokers, providers, and underwriters may impact negotiation of insurance coverages or caps
  - Not recommended to tie liability caps to amount of insurance
  - Some coverages, brokers, or underwriters may prohibit designating third parties as “additional insured” or providing a “waiver of subrogation”

VENABLE LLP

Tips & Takeaways

VENABLE LLP

Tips & Takeaways

1. Understand the deal before review, including processing roles, services, deal value, and data in scope
   - Review in tandem with the MSA/underlying agreement wherever practical
2. Be reasonable where you can!
   - Consider the practicality of specific DPA terms when drafting and negotiating, especially with respect to terms with real operational impacts, like subprocessor engagements, audit rights, and detailed security exhibits
   - Work hand in hand with business and risk management teams when negotiating significant risk allocations like indemnities, liability caps, etc.
3. Create templates, checklists, and/or playbooks with pre-approved fallbacks
4. Identify and create formal escalation processes for common issues
5. Get knowledgeable help if you need it

VENABLE LLP

Questions?

VENABLE LLP

VENABLE LLP