November 2022

Working with Service Providers & Third Parties in 2022

Beatrice Botti
VP, Global Data & Privacy Officer
DoubleVerify

Kal Dhinsa
Chief Information Security Officer, NDVR

Meredith Halama
Partner, Perkins Coie LLP

Privacy+ Security Forum

Speakers

Beatrice Botti
VP, Global Data & Privacy Officer
DoubleVerify

Kal Dhinsa
Chief Information Security Officer
NDVR

Meredith Halama
Partner
Perkins Coie LLP

General Considerations When Working with Vendors

Privacy+ Security Forum

Backing Up: Working with Vendors before 2018

Privacy+ Security Forum

Legal Requirement: "Reasonable Security":

- Section 5 of FTC Act
- Various Sectoral Laws
- State security laws
- Tort liability
- SEC safeguard rules
- GLBA
- And others…

Practical/Commercial Considerations:

- Don't want your providers selling your data, or using it for their own purposes
- Breaches cause reputational concerns even where not legal consequences

What Does Reasonable Security Mean?

Privacy+ Security Forum

When working with others, generally:

1. Minimum standards for service providers (tiered by sensitivity of the data they held or criticality of the service)
2. Due diligence process that allows sufficient understanding of the vendor's practices in order to assess it against minimum requirements
3. Periodic assessment/audit of the third party
4. Contractual language that is tied to the identified minimum control requirements.

GDPR Starts to Change the Game

Privacy+ Security Forum

Article 28 Dictates Rules for Working with Processors

Privacy+ Security Forum

Contract with Processor Must:

- Require the processor to process only on controller's documented instructions
- Ensure that people authorized to process have committed themselves to confidentiality
- Secure the data in accordance with with requirements of the GDPR and assist in breach reporting
- Disclose and have consent for any subprocessors used
- Require the processor to assist in facilitating controller's obligations with respect to the data subject's rights
- Return or destroy data after the end of the provision of services
- Makea available to the controller "all information necessary to demonstrate compliance with" Art. 28 and "allow for and contribute to audits."
- Inform the controller if, in the processor's opinion, the controller's instruction inferences on the GDPR or other law

Working with Other Controllers Under the GDPR

Privacy+ Security Forum

No equivalent of Art. 28 for sharing with other controllers, but assists controller in meeting its obligations by:

- Maintaining legal bases for processing
- Ensure data is not processed in manner incompatible with the purposes specified when the data was collected and that processing is limited to what's necessary in relation to purposes for which the data was collected
- And more…

Virginia, Colorado, Connecticut, and Utah

Privacy+ Security Forum

Obligations for Working with Processors in the Non-California States

Obligations Similar to the GDPR, Including:

- Clearly set forth the instructions for processing, including: (1) Nature and purpose of processing, (2) Type of data subject to processing, (3) Duration of processing, and (4) Rights and obligations of both parties.
- Impose a duty of confidentiality on the processor.
- Require the processor to:
  - Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
  - Pass on obligations to subprocessors via written contract (with CO and CT requiring an opportunity for the controller to object, and CA requiring notice).
  - Delete or return (at controller's direction) PI at the end of the provision of services unless retention is required by law.
  - Make available to the controller all information necessary to demonstrate compliance with the law.
  - Allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor (audit provisions vary across the laws).
  - Assist the controller with certain obligations, including in responding to and complying with consumers' rights requests.

And Then Came the CCPA, and then the CPRA

Privacy+ Security Forum

Who's Who Under the CPRA

Privacy+ Security Forum

Service Provider

A person that processes PI on behalf of a business and which receives PI from or on behalf of a business for a "business purpose" pursuant to a written contract that makes specific commitments.

Contractor

A person to whom the business makes available a consumer's PI for a "business purpose" pursuant to a written contract that makes specific commitments.

Third Party

A person who is NOT (1) the business with whom the consumer intentionally interacts and collects PI from the consumer as part of this interaction, (2) a service provider, or (3) a contractor.

Service Provider & Contractor Agreements - Restrictions

Privacy+ Security Forum

Under CPRA, Contracts Must Prohibit the Service Provider or Contractor From:

- Selling or sharing the PI
- Retaining, using or disclosing PI for any purpose other than for **business purposes** specified in the contract (*and the "limited and specified" business purpose must be set forth in the contract*);
- Retaining, using, or disclosing PI for any commercial purpose other than the business purpose specified in the contract
- Retaining, using, or disclosing PI outside of the direct business relationship between the service provider and the business - *for example, by combining or updating personal information received pursuant to the the contract with personal information received from other sources or its own interactions with the consumer*

Also note: service providers and contractors cannot engage in cross-context behavioral advertising

Service Provider & Contractor Agreements - Obligations

Privacy+ Security Forum

Audit Rights

A business must have the right to take "reasonable and appropriate steps" to ensure that the service provider or contractor uses the personal information consistent with the business's obligations, including "ongoing manual reviews and automated scans" and regular internal or third party assessments, audits, or other technical or operational testing at least once every year

Subprocessors

If the service provider or contractor engages another person to assist it in processing PI for the business, it must flow down the same contractual commitments via a binding written agreement

Comply with Law/Assist with Consumer Requests

Service providers and contractors must comply with law, may be required to cooperate with businesses in responding to verifiable consumer requests and to protect personal information, and notify the business if they cannot meet their obligations. Also must enable business to comply with consumer requests.

But What Are Business Purposes?

Privacy+ Security Forum

"Operational" and Other "Notified Purposes," Including:

- Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance.
- Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.
- Debugging
- Short-term, transient use, including, but not limited to, **non-personalized advertising**
- Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.
- Providing advertising and marketing services, **except for cross-context behavioral advertising**,
- Internal research for technological development and demonstration
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

Due Diligence, Oversight, and Remediation

Privacy+ Security Forum

CPRA Demands Due Diligence And Oversight for Service Providers and Contractors:

- Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the law.
    - For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the law
- Contract must grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider or contractor's unauthorized use of personal information.
    - For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.

Security & Breach

Privacy+ Security Forum

CCPA Also Penalizes Breaches:

- Civil Relief: Any consumer whose nonencrypted and non redacted personal information (as defined by California's breach law) or whose email address in combination with a password or security question and answer that would permit access to the account, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may recover damages ($100-$750) per incident or actual damages or injunctive relief.
- Regulatory enforcement: Any business, service provider, contractor or other person that violates the CCPA subject to administrative fines of $2,500-$7,500 (for intentional violations)

Practical Considerations For Working with Third Parties

Privacy+ Security Forum

Balancing Legal & Practical Considerations

Privacy+ Security Forum

Contractual Relations

Legally

- Merchant must bind vendors to standards that apply including PCI
- Responsible for their compliance
- Regulators expect due diligence for sensitive data handling; need both contractual terms and risk assessment

Practically

- Large vendors have comparative advantage, resources for better security than most merchants
- Large vendors have higher compliance burdens and corporate incentive to avoid breaches
- Bargaining power can be limited to what they have decided to offer

Sample Vendor Approval Flow