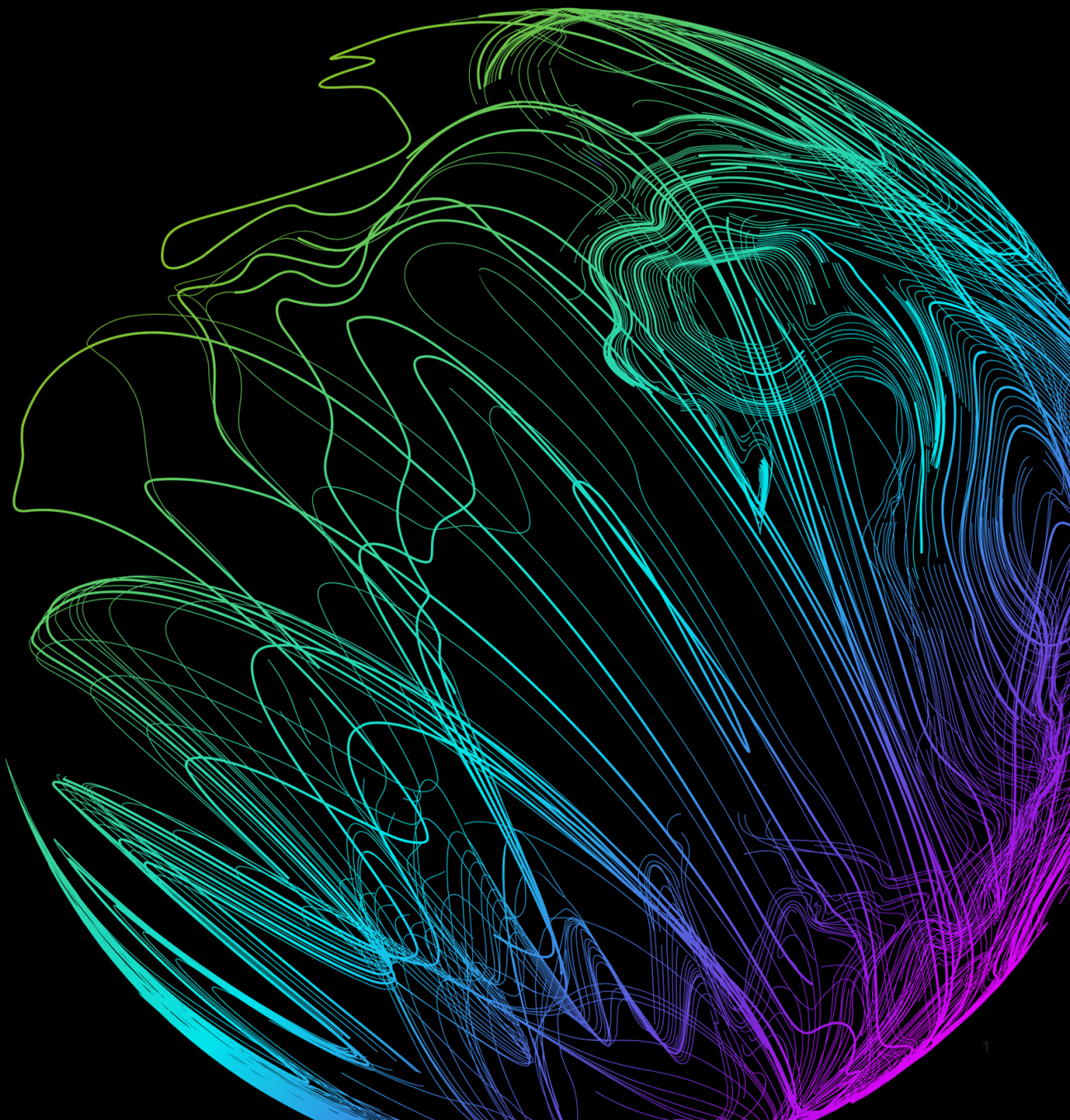
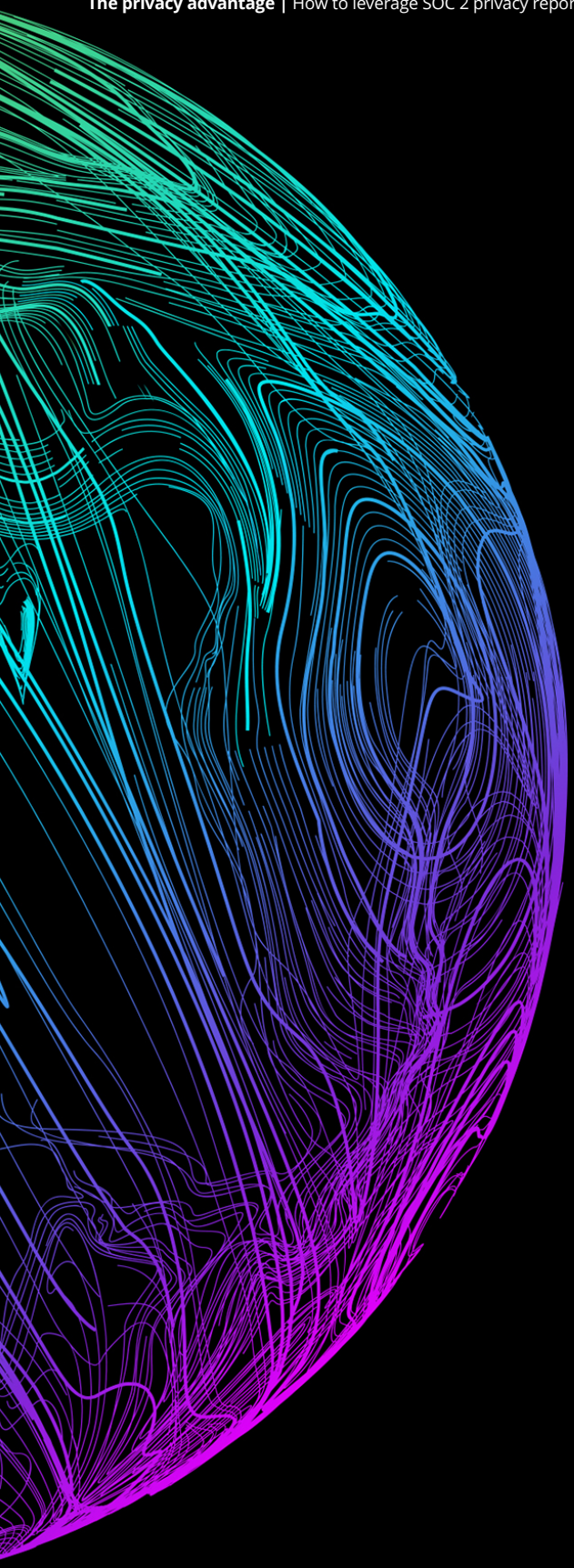
Deloitte.

The privacy advantage

How to leverage SOC 2 privacy reporting for competitive advantage





Researchers have traced the origins of outsourcing as a business strategy back to the 1950s.[1] Of course, in those simpler times, the practice differed significantly from today. Contracted services were generally limited and straightforward—publishers outsourced printing services, property managers contracted for janitorial services, banks obtained security services, and so on. Agreements were basic, if not a handshake; the voluminous exchange of personal data was rare; performance metrics were simple; and the contracting parties were satisfied if one executed as expected and the other paid as agreed.

More notably, in the 1950s, the administrative burdens placed on outsourced service providers (OSPs) were minimal. Regulatory oversight was scant: Privacy laws and regulations such as the EU General Data Protection Regulation[2] (GDPR) and the California Privacy Rights Act[3] (CPRA) were decades away from being enacted.

Fast-forward 70 years, and the range of services performed by OSPs has expanded exponentially, perhaps exceeded only by the legal and regulatory requirements they are subject to. In the 21st century, OSPs must satisfy the needs of multiple stakeholders—customers, investors, board members, regulators, insurers, and more—all of whom seek comfort and surety over their data privacy controls, and many of whom require formal, written, auditable assurance of the same.

These myriad obligations are not likely to ease anytime soon. Comprehensive privacy regulations are becoming progressively more prevalent in many jurisdictions throughout the world. In the United States in particular, individual states increasingly have privacy on their radar. Since the California Consumer Privacy Act (CCPA) was strengthened by CPRA in 2020, numerous states have followed suit with privacy regulations of their own, including Colorado, Connecticut, Utah, and Virginia, with more expected to follow.[4] For OSPs—whether operating regionally, nationally, or internationally—tracking and adhering to this multitude of requirements has become commensurately complex and onerous.

Outsourced risk?

It's something of a mantra in the outsourcing world that "a process can be outsourced, but the associated risk cannot." In other words, if a consumer's data is lost by an organization due to a controls failure at its OSP, the consumer holds the organization accountable—not the OSP.

This would seem to get the OSP off the hook, but unfortunately, the mantra doesn't stand up to scrutiny. While it's true that the "controller" (see sidebar, "Privacy players") often takes the blame for data breaches and shoulders the risk of getting fined by regulatory bodies if the "processor" does not properly handle consumer data, in some jurisdictions, both the controller and the processor can be fined.

In addition to regulatory sanctions, the processor can suffer immediate and long-term reputational damage for mishandling data, as well as potential breach-of-contract lawsuits and other consequences.

As a result, many processors have learned the hard way that, contrary to conventional wisdom, risk can indeed be outsourced, and their customers' vulnerabilities quickly become their own.

The organizations that processors serve (i.e., an OSP's customers) face compounding risks, including increased reliance on technology, intensifying regulatory scrutiny, and escalating cyberthreats, all of which compel them to badger their processors with information requests. Unfortunately, the depth and breadth of information being requested is often inconsistent and unclear—and not always readily available—leaving the processor scrambling to respond in an efficient and timely fashion.

Response mechanisms

When the controller comes knocking, the processor must open the door. Yet deciding exactly what to provide, as well as when and how to supply it, plagues many processors. Varying approaches are employed, and inconsistent or unsatisfactory results often manifest. The scope, frequency, and assurance levels of these mechanisms are frequently challenging, sometimes cost-prohibitive, and—in some instances—insufficient in providing meaningful assurance. The following are some common response mechanisms.

Privacy players

Who's who in the world of data privacy

Three primary players inhabit the world of data privacy.

Data subjects (e.g., customers, consumers, and clients) share their personal information in the course of an interaction or transaction.

The organizations that request said information and determine the purpose and means of data processing are known as **controllers**.

And the entities that process personal data, such as outsourced service providers, are referred to as **processors**.

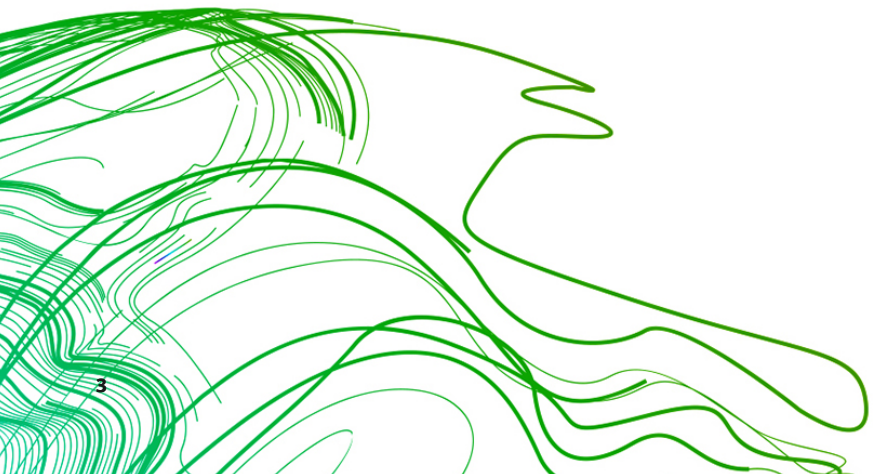
While an organization may control and process personal data, in many cases controllers will outsource processing of personal data to a third-party processor. Examples of this include using processors to perform payroll administration, handle statement printing, or provide cloud applications

Methods of Assurance

Service organizations have a variety of methods to provide their stakeholders with assurance. SOC 2 privacy reporting provides the ability to satisfy many users and provide a high level of assurance.

Assurance method	Description	Scope	Level of assurance
Standard controls statement/attestation from management	Typically, a short narrative that describes the controls environment for a broad set of risk and control domains applicable to the general control environment.	Generally broad	Low
Industry-accepted domain-specific questionnaire	A standardized questionnaire, usually maintained by an industry forum, that covers specific risk areas and controls along with some details of how they are implemented and supported by evidence documents (e.g., policies, procedures).	Generally broad	Low
Organization-specific surveys	Usually, lengthy questionnaires sent to the OSP to report on its own level of internal control maturity.	Generally broad	Low
Targeted certification	The processor OSP achieves certification in some chosen standard, for example, ISO27001 or ISO9000.	Limited and may not be frequent	Moderate
Individual customer audits	Risk management or internal audit resources from the controller organization are sent to the processor OSP to perform walkthroughs and testing procedures.	Varying, and not likely frequent	High
System and Organization Control (SOC 2) privacy reports	The operating effectiveness of controls is tested using a strict audit methodology. The attestation vendors providing these independent assessments are generally larger audit companies with access to the necessary competence to deliver all aspects of the assessment with stringent quality control standards.	Generally annual; adheres to customers' requirements	High

A SOC 2 examination reports on whether controls were effective to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria (e.g., privacy).



SOC 2 privacy reports

Based on our experience working with OSPs, along with our familiarity with the commonly used response mechanisms, we consider obtaining a SOC 2 privacy report to be a leading practice.

SOC 2 privacy reporting offers an efficient, streamlined approach for satisfying customer inquiries, questionnaires, audits, regulatory compliance concerns, and more as it relates to data privacy. The reports provide an internationally recognized way for processors to supply their customers—and their customers' auditors—with an objective opinion on the effectiveness of the control environment.

What makes the SOC 2 report appealing? Primarily, its rigor. The independent service auditor report describes a standardized set of control criteria that are stringently tested, providing assurance that the controls are:

- Properly designed to meet agreed-upon control criteria
- Implemented as intended
- Operating effectively over a specified time period

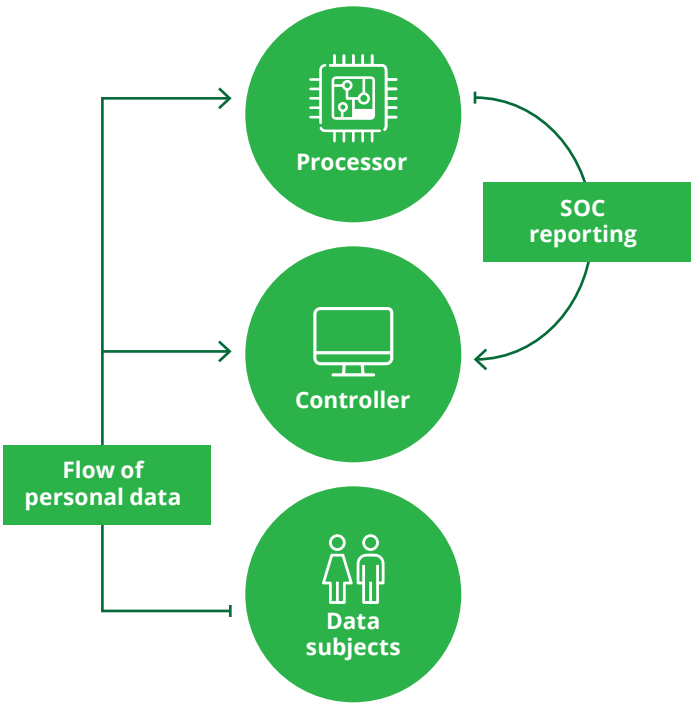
Flow chart for SOC 2 privacy reports

As previously described, a processor is an entity that acts as an OSP, processing personal data on behalf of the controller.

As processors do not determine the purpose and means of processing, and may not interact directly with the data subject, a smaller subset of privacy requirements commonly apply to them. Relevant privacy requirements typically include limiting the use of data as appropriate, only retaining the data for as long as necessary, and properly disposing of the data once it is no longer needed. The SOC 2 privacy report provides assurance to the controller that the processor has the right controls or mechanisms in place to protect the data.

In the flow chart that follows, data subjects send personal data to various entities. Entities that collect personal data are commonly controllers; however, data may be collected directly to a processor (e.g., a payment processor acting on behalf of a utility company). Each of these entities is responsible to comply with relevant privacy requirements. A SOC 2 privacy report provides controllers with assurance that they are outsourcing processing to a service provider that has controls in place to comply with relevant privacy requirements. The report provides an understanding of controls in place at the processor and any exceptions in the design or operating effectiveness of controls in the processor's privacy control framework.

SOC 2 privacy reporting



Transformative transparency

One critical component of a successful outsourcing relationship is "outsourcing transparency": clear, timely, and open communication between the two parties on priorities and information requirements.

Processors can attain increased transparency by streamlining and structuring reporting requirements into an integrated risk and controls framework, with the goal of becoming more efficient and cost-effective while better meeting the needs of their customers.

Several approaches are available to help processors develop a baseline for customer requirements, including reviewing existing contracts, holding focus groups, monitoring industry trends, conducting internal audit site visits, and executing questionnaires.

Once the baseline is established, processors can identify gaps in controls and processes across their organization and flag inconsistencies in communication with their customers. Then, rather than providing an ad hoc response each time an information request comes in, processors can deliver—in a timely and efficient manner—an independent audit report that is mapped to the specific needs of the customer and that can stand up to regulatory scrutiny.

The effort can be transformative for the processor organization, converting a cumbersome, sluggish, and expensive process into one that delivers a high level of assurance at a lower cost. The benefits can then cascade: happier customers, a burnished reputation, growing market share, and improved margins.

Or, as we like to call it: "The privacy advantage."

Privacy permutations

Fundamental changes are taking place in today's privacy marketplace.

Evolving regulatory landscape: Since the introduction of GDPR in 2018, a multitude of new data protection regulations has disrupted core sectors.

COVID-19 repercussions: The ongoing pandemic has forced companies to expand their digital footprints to preserve connectivity and business profitability, increasing the risks to user privacy.

Increased consumer awareness: Gaining privacy-conscious consumers' trust has been challenging for many organizations. Consumer-facing businesses without transparent communications around privacy can create confusion in the market, further deteriorating consumer confidence.

Enhanced consumer protections: Globally, consumers are being provided with new protections and rights with new privacy regulations, either enacted or under consideration.

Ineffectual privacy compliance: One-off approaches to privacy compliance have resulted in narrowly focused, scattered, or siloed privacy initiatives, creating operational and financial constraints, particularly for businesses with a global footprint.

SOC 2 specifics

SOC 2 privacy reports address the privacy of personal information that a service organization collects, uses, retains, discloses, and disposes of for user entities.

The AICPA defines personal information as nonpublic information about or related to an identifiable individual, such as personal health information or personally identifiable information (such as personnel records, payment card information, and online retail customer profile information).

The AICPA's privacy trust service criteria relates to the following areas:

- Notice and Communication
- Choice and Consent
- Collection
- Use, Retention, and Disposal
- Access
- Disclosure and Notification
- Quality
- Monitoring

Contacts

Sara Lademan
Partner | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
slademan@deloitte.com
+1 312 486 2981

Carolyn Axisa
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
caxisa@deloitte.com
+1 212 436 2820

Mendy Phillips
Senior Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
menphillips@deloitte.com
+1 212 266 4295

Endnotes

1. Daniel Usifoh, "Outsourcing: A brief history," Gateway Procurement, accessed October 4, 2022; Supply Chain Resource Cooperative (SCRC), "A brief history of outsourcing," June 1, 2006.
2. GDPR.EU, "What is GDPR, the EU's new data protection law?," accessed October 4, 2022.
3. Californians for Consumer Privacy, "California Privacy Rights Act: Executive Summary," accessed October 4, 2022.
4. F. Paul Pittman, Kyle Levenberg, and Shira Shamir, "Data protection laws and regulations USA," Data Protection 2022 (London: Global Legal Group, 2022).

Deloitte.