A Practical Data Privacy and Security To-Do List for 2023

Todd Daubert
Dentons US LLP
Washington, D.C.
todd.daubert@dentons.com
202.408.6458

William Krouse
Dentons US LLP
Washington, D.C.
william.krouse@dentons.com
202.496.7076

Jacqueline Scott
Dentons US LLP
New York City
jacqueline.scott@dentons.com
212.398.3891

Agenda

- ✓ Overview – Roadmap for Action in 2023 and Key Dates for US State Privacy Laws
- ✓ Practical Data Privacy and Security To-Do List for 2023
- ✓ Key Takeaways
- ✓ Questions Throughout

Practical To-Do List for Data Privacy and Security

Roadmap for Action in 2023

1. Review how you are **collecting** information, and how much of the information you collect is personal or sensitive
2. Review how you are **using** the information you have collected
3. Review how you are **sharing** personal or sensitive information with third parties
4. Review how you are **protecting** information, including personal or sensitive information, by assessing your data security policies and practices
5. Review your **strategic approach** to information and identify:
   a) improvements that could increase revenue and/or reduce risk; and
   b) changes that are necessary to be compliant with applicable law

2023 Is the Right Time for Adopting a Broader Perspective

Many benefits to expanding focus beyond current mandates

- California and Virginia have taken the lead with respect to new mandates in 2023, but Colorado, Connecticut, and Utah also have new mandates for 2023
  - The amendments to the California Consumer Protection Act (CCPA) by the California Privacy Rights Act (CPRA)[1] became effective on **January 1, 2023**
    - Additional obligations surrounding the collection and usage of Sensitive Personal Information, a new category of data
    - Additional privacy rights granted to consumers (right to correct, right to limit use of Sensitive Personal Information)
    - Additional control over sharing personal information with third parties for cross-context behavioral advertising
    - Created a new, dedicated privacy regulatory authority (CPPA) responsible for enforcement
  - The Virginia Consumer Data Protection Act (VCDPA)[2], which incorporates many of the CPRA's principles, became effective on **January 1, 2023**, with enforcement beginning on July 1, 2023, including similar:
    - Applicability thresholds (*e.g.*, process over 100,000 Virginia residents' personal information)
    - Service provider and vendor contractual requirements to protect personal information being processed
    - Data subject privacy rights (*e.g.*, access, deletion, correction, sale and targeted advertising opt-outs, etc.)
- These new mandates both reflect and affect the expectations of consumers and regulators throughout the United States, and more states are likely to follow
- Accordingly, all companies should consider adopting a **holistic and strategic approach** to personal information that reflects consideration of these new mandates in order to foster trust with consumers, improve revenues, reduce risk, and improve efficiency

[1] *Cal. Civ. Code §§ 1798.100 to 1798.199.100*

[2] *Va. Code Ann. §§ 59.1-575 to 59.1-585*

Key Dates for US State Privacy Laws

2023 Compliance Deadlines

	California Privacy Rights Act (CPRA) that Amends the CCPA	Virginia Consumer Data Protection Act (VCDPA)	Colorado Privacy Act (CPA)	Connecticut Data Privacy Act (CTDPA)	Utah Consumer Privacy Act (UCPA)
Effective Date of Law	January 1, 2023	January 1, 2023	July 1, 2023	July 1, 2023	December 31, 2023
Date Compliance Must Begin (Lookback Period)	January 1, 2022 1 year lookback	January 1, 2023 No lookback	July 1, 2023 No lookback	July 1, 2023 No lookback	December 31, 2023 No lookback
Date Enforcement Begins	July 1, 2023	July 1, 2023	July 1, 2023	July 1, 2023	December 31, 2023
Cure Period following Notice of Violation	30-Days, but only for security breach violations	30-Days	60-Days until January 1, 2025	30-Days until December 31, 2024	30-Days

Review the Types of Personal Information You Collect

Definition of Personal Information Is Evolving and Expanding

- California has changed, and broadened, the definition of personal information
  - Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household (*Cal. Civ. Code § 1798.140(v)(1)*)
  - Please also note that the previous exemptions for employee and business-to-business information expired on January 1st, 2023
- Some types of information become personal information (or sensitive personal information) only when **combined** with other types of personal information
  - For example, precise geolocation, ethnicity, religious beliefs, and positive test results are non-personal information until they are combined with other personal information, at which point they become sensitive personal information
- The definition of personal information may vary – even within the same state – based on the purpose of the law that contains the definition
  - For example, the definition of personal information that triggers a mandatory breach notification in California is narrower than the definition for other purposes (*Cal. Civ. Code § 1798.82*)
- Consider the impact of statutory **exclusions** to personal information
  - For example, publicly available information and anonymous/de-identified or aggregated data
- Understanding the personal information that you collect (*e.g.*, **data mapping**) is critical for understanding your legal obligations, business opportunities, and risk

Review the Types of Sensitive Personal Information You Collect

Sensitive Personal Information is subject to more obligations

- Some states, including California, Connecticut, Utah and Virginia, have created a new category of personal information – **sensitive personal information** – that is subject to additional obligations and protections
- Sensitive personal information typically includes:
  - Financial account information
  - Data about a consumer's government-issued identifications
  - Contents of a consumer's **electronic communications**
  - Precise **geolocation** data
  - Data collected from a **child**
  - Citizenship, immigration status, and union membership
  - Information concerning a consumer's sex life or sexual orientation
  - **Biometric** data
- Understanding the additional risks and obligations associated with the sensitive personal information you collect is critical
  - For example, California requires businesses to honor requests to limit the use of sensitive personal information to that which is strictly necessary,[1] and Virginia prohibits the processing of sensitive personal information without the individual's consent[2]
  - In December, the FTC announced two separate settlements for more than $500 million against the developer of "Fortnite" for violations related to the collection and use of children's data.

[1] *Cal. Civ. Code § 1798.121*

[2] *Va. Code Ann. § 59.1-578(A)(5)*

Review How You Are Collecting Personal Information

Personal information can be collected in several ways

- The only way to verify that your privacy disclosures, notices and protective measures are accurate and appropriate is to identify and review each of the means by which you collect personal information
  - Direct Collection
    - Customer forms
    - Contact information for customers and other business representatives
    - Notes or recordings of discussions with third parties
    - Cookies
    - Orders
  - Indirect Collection
    - Personal information provided by third parties like vendors, business customers, business partners, advertisers

- Carefully consider and review **joint collections** of personal information with a third party
  - When jointly collecting personal information, allocate responsibility between first- and third-party disclosures, and ensure disclosures are accurate

- Consider also the **purpose** for which you are collecting personal information, which will impact your privacy disclosures, notices and protective measures

Review How Your Are Using Personal Information

Pay particular attention to any changes in usage

- Take inventory of the ways in which you are using personal information
- Review whether the identified uses are accurately described in privacy notices and disclosures
- Consider whether disclosures and notices provided at the time of collection remain accurate after any changes in usage since collection
- You may be subject to additional **purpose specification and limitation** requirements under Virginia's new data privacy law (*Va. Code Ann. § 59.1-582*)
- Consider applicable **use limitations** for types of personal information
  - Is **consent** required before processing certain sensitive personal information?
  - Implement a **privacy-by-default** approach for children's data
  - Carefully consider whether to use AI/machine learning as consumers have the right to stop **automated decision-making** and **profiling**
- Consider the importance of implementing and honoring **data retention** policies and procedures to comply with data minimization requirements (*Cal. Civ. Code § 1798.100(a)(3)*)

Update Disclosures, Policies, and Practices

Pay particular attention to any changes in usage

- Update disclosures and notices to ensure accuracy and to reflect necessary use limitations
- Consider when **consent** is required before using sensitive personal information
  - Implement a consent manager that solicits consent *before* the processing begins as well as opt-out mechanisms if consumers change their mind
  - Review whether reliance on consent in the United States creates issues for other jurisdictions like the European Union
- Review and, as necessary, amend or implement operational procedures, especially around biometric and sensitive personal information
  - Prepare valid opt-out mechanisms (*e.g.*, "Limit the Use of My Sensitive Personal Information" link) and to receive opt-out signals (*Cal. Civ. Code § 1798.135(b)*)
  - Failure to provide proper disclosures when collecting biometric information can result in hefty court damages and regulatory fines (see *Rogers v. BNSF Railway*, where truck drivers won a $228 million judgement)
- Prepare required regular **data processing/protection impact assessments**, and consider them even when not required
  - Consider a "global" approach to address the various state requirements in order to account for all applicable risks

Review How You are Sharing Data

Some state definitions of “Sale” and “Share” are very broad

- Numerous organizations are likely “selling” and/or “sharing” personal information due to the terms’ broad definitions

- Take **inventory** of the ways in which you are disclosing personal information to third parties (including affiliates)

- Ensure that such disclosures are **consistent** with applicable law
  - Why is the information being disclosed in the first place?
  - What is the end goal for disclosing the data?
  - What are the legal and practical protections you must put in place before disclosing?

- Monitor and control all data flows with third parties to avoid **data leakage**
  - Your organization may ultimately be held responsible for the actions of third parties with which you have shared personal information

- In August, Sephora was fined $1.2 million by the California AG for failing to disclose to consumers that it was selling their personal information and failing to honor sale opt-out requests (*People v. Sephora United States,* No. CGC-22-601380 (Cal. Sup. Ct. Aug. 24, 2022))

Update Disclosures, Policies, and Practices Regarding The Sale or Sharing of Personal Information

- **Inform** individuals of whether your organization sells or shares personal information and that they have the right to opt out
  - Review the targeted and behavioral advertising, if any, your organization conducts, including the website's use of cookies and other tracking technology

- Consider implementing clear and simple **intake methods** for requests relating to personal information so that individuals can efficiently and easily exercise their rights, and you can build consumer trust and manage requests efficiently

- When engaging in selling or sharing, implement **opt-out mechanisms** that are simple and easy to use for the average consumer
  - For example, California explicitly requires companies to create a **"Do Not Sell or Share My Personal Information"** portal with a link in the footer of your website (*Cal. Civ. Code § 1798.135(a)(1)*)

- Maintain detailed customer request and opt-out **records** as evidence that your organization is taking compliance seriously

- Provide adequate **training** to individuals responsible for handling privacy rights inquiries and processing opt-out requests

Review or Implement Required Opt-Out Mechanisms and Global Privacy Controls For Data Sharing

Update Functionality To Comply With New Requirements

- The exact location of **opt-out right notices** may depend on your organization's operation methods
  - For example, Webpage link; Standalone notice; Mobile app; Offline method
- The California, Colorado, and Connecticut regulations contemplate an **electronic opt-out signal**[1]
  - As you look to third party tools and technologies to implement opt-out mechanisms, continue to monitor these regulations
- Maintain a process to reconcile situations where an individual's opt-out signal conflicts with such consumer's preferences previously shared
- Avoid enforcement agency attention by **honoring opt-out and other individual requests**
  - Failure to comply with these requirements not only puts your organization at risk for **hefty fines** but also diminished **brand reputation and value**

[1] Cal. Civ. Code § 1798.185(a)(19); Colo. Rev. Stat. § 6-1-1306; CTDPA, S.B. 6, Gen. Assemb., Reg. Sess. (Conn. 2022), Sec. 5.

Review and, if necessary, Amend or Update Vendor Agreements

Increased Third-Party Compliance Obligations

- The new privacy laws in California, Colorado, Connecticut, Utah, and Virginia all require a **written agreement** to be executed with the vendor or service provider if the vendor or service provider will process personal information

- Perform an **"internal audit"** to identify your organization's vendors and to better assess their contractual requirements based on their roles
  - Service providers
  - Contractors
  - Third parties

- Where necessary, amend or update vendor agreements with a particular focus on cooperation in responding to **data subject requests** as well as **breach notification** responsibilities and risk allocation

- Consider performing third-party **due diligence** and regular **audits** to ensure the security measures taken by your vendors are sufficient to meet new data protection standards (Va. Code Ann. § 59.1-579)

Review How You Are Protecting Data

Assess Your Data Security Policies and Practices

- Data security rules have become stricter and more complicated as new regulations are implemented
  - Additional operational requirements, including **data protection/risk assessments**
  - Updated data **incident reporting** requirements
  - Enhanced requirements around data security **safeguards**

- Data protection requirements will also vary widely based on the type of information involved
  - *E.g.*, Sensitive personal information; Children's data

- Conduct regular **impact assessments** to evaluate the protection of certain information in view of your data processing activities

- Where possible, develop a **"global" privacy program** that can broadly satisfy common requirements across various state laws

- **Monitor enforcement activity** across all jurisdictions to better understand enforcement trends and expectations

Update Policies and Practices To Ensure That You Are Protecting Data In Accordance With Applicable Law

- Review existing data security documentation and processes to determine what changes may be needed to achieve compliance with the new laws
- Understand and implement **industry best practices**, such as those provided in the NIST Cybersecurity Framework
- Conduct and document regular risk assessments/audits to help meet the **“reasonable” standard** of data security measures
- Work with IT departments to build and maintain **strong critical infrastructure** to minimize security incidents and data leaks
- Properly **document** data protection policies and practices to help ensure proof of compliance
- Take note of **heightened FTC scrutiny** when implementing data security policies and procedures

Incorporate Strong Data Strategies To Increase Revenues and Reduce Risk

Consider Changes To Your Current Approach

- Review how your organization views data and how its current approach aligns or departs with data trends in the US and around the world
  - Transparency is a top priority
  - Consumers are exercising their rights
  - Rise in privacy enforcement

Strategies To Increase Revenue and Reduce Risk

- Drive customer loyalty and trust by being **transparent** with your data practices
- Maintain brand reputation and value by making **data protection** a top priority
- Reduce the risk of data breaches and improve strategic decision-making by **optimizing data**
- Manage information security risks by setting risk expectations and guidelines and conducting regular **training** to employees and vendors

Approach Data Privacy and Security Compliance Holistically

Not Merely A Costly Compliance Obligation

- The risk landscape for organizations has changed significantly over the years as new and evolving regulations come into effect

- Explore structural and systematic means for ensuring that approaches to data are consistently evaluated **holistically** throughout your organization
  - Assess your organization's needs by performing data **due diligence** to understand root causes of data issues
  - Articulate how data will help achieve your organization's overall **business goals** and outcomes
  - Extend compliance across **all aspects of an organization**: people, places, processes, and products
  - Compliance is an evolving process that requires **ongoing commitment**

Key Takeaways

Setting Up A Successful 2023 And Beyond

- Focus on **data mapping** exercises in order to account for and subsequently manage all information that falls under the expanded definitions of personal and sensitive information

- Update/develop **policies and procedures** around collecting and using data, including responding to consumer rights, impact assessments, data retention, and record keeping

- Conduct **security breach preparedness** exercises and review/update your information security program plan

- Ensure a **holistic approach** to data compliance by making data governance a company-wide effort

Questions?

大成 DENTONS

Trending Workplace Issues: Creative (and Legal) Solutions

January 25, 2023

Grow | Protect | Operate | Finance

Remote & Hybrid Work

Legal Consideration: Fair Labor Standards Act (and state corollaries)

Facts: The number of American workers who work primarily from home has **quadrupled** since 2019.
As of 2022, 26% of American workers work primarily or exclusively from home.
Only 11% of employers use all of the office space they have access to.
6% of employers have reduced their square footage since 2020.

Example: Employee moved to California and did not notify employer.

Issues: Applying state law requirements (i.e. worker's comp, varying paid sick leave and pay upon termination rules)
Timekeeping
Compensable time

Solution: Designate employee's workplace and the state law that applies, as a condition of employment.
Require employees to use timekeeping software.
Create clear policies about emailing "off the clock" and commuting.
Confirm compliance when there is a move (see Paid Sick Leave slide, for example).

Employee Mental Health

Legal Consideration: Americans with Disabilities Act

Facts: In 2020, NAMI reported that 1 in 5 adults in the US experience mental illness, with 1 in 20 being “serious”.

People with depression have a 40% higher risk of developing cardiovascular and metabolic diseases.

32.1% of US adults with mental illness have also experienced a substance use disorder.

1 in 5 US adults report that the pandemic had a significant impact on their mental health; higher reports from individuals with pre-existing mental illness.

Calls to national mental illness hotlines increased by 70% during the pandemic.

Example: Employee experienced a mental break and disclosed sensitive information about a customer to the public.

Issues: Complying with the Americans with Disabilities Act (ADA)

Workplace safety and data security

Keeping the “human” in Human Resources functions

Solution: Revise policies and procedures to comply with the ADA.

Upgrade safety and security protocols.

Train managers to recognize and address mental health issues in the workplace.

Low Unemployment

Legal Consideration: Employee Perks and Benefits

Facts: Current rate of unemployment as of November 2022 is 3.7%, down from 14.7% at the height of the shutdown.

Pay rates expected to increase an average of 3% in 2023 (after an average increase of 4.9% in 2022).

The size of the labor force (people looking for or in jobs) has fallen to 62%, representing millions of would-be workers.

There are two jobs for every one person looking for a job.

Example: Employer increases benefits (like “unlimited” PTO).

Issues: Complying with non-discrimination requirements in benefits plans and employment practices.

Balancing aggressive hiring policies with practical management and long-term sustainability.

Confirming compliance with state requirements.

Solution: Identify the changing needs of the labor market as applied to <u>your</u> business.

Maintain hiring, conduct, and performance standards while addressing barriers to employment.

Work From Home

Legal Consideration: Americans with Disabilities Act

Facts: According to the Department of Labor, In December 2022, 39% of the population of disabled people was either working or actively looking for work. This is compared to 76.9% of the population of people without disabilities.

Example: Prior to the COVID pandemic, an employee with a disability requested reasonable accommodation of working from home and presented a disability-related need for the accommodation. The reasonable accommodation was denied because the employer was concerned they would not be able to perform essential job functions while working from home. During the COVID pandemic, employees worked from home. Upon returning to the office, the same employee with the disability now requests to work from home.

Issues: Pre-pandemic: “As an initial matter, there is general consensus among courts, including ours, that regular work-site attendance is an essential function of most jobs.” *Credeur v. Louisiana*, 860 F.3d 785, 793 (5th Cir. 2017).

Today: “This is not to say that every job requires in-person attendance. This Court recognizes that remote work is a regular part of many different fields, a reality that has grown even more prevalent since the Covid-19 Pandemic.” *Turner v. Bd. of Supervisors of the Univ. of La. Sys*., 2022 U.S. Dist. LEXIS 174485, at *20 (E.D. La. Sep. 27, 2022)

Temporary telework experience could be relevant to considering the renewed request.

Solution: Re-engage in the interactive process.

Consider whether employee with disability could satisfactorily perform all essential functions while working remotely.

Diversity & Inclusion

Legal Consideration: **ESG** + Title VII and Age Discrimination in the Workplace

Facts: Women comprise 58% of the workforce.

People aged 55 and over represent the largest portion of the workforce by age.

White candidates are more likely than Black candidates to receive an interview call-back.

White and Asian employees make, on average, $637 more per week than Black and Hispanic employees.

EEOC Charges alleging Race, National Origin, and Color discrimination increased in % in 2021.

37% increase in social shareholder proposals in 2021 compared to 2020.

Issues: Social and political demand for diversity and inclusion initiatives not translating to a decline in workplace disparities along the lines of race, gender, ethnicity, etc.

Solution: Policies, procedures, practices, documentation, and training that align with ESG initiatives.

Develop leadership pathways.

Legalization of Cannabis

Legal Consideration: Employee Drug Testing

Facts: Federal law still bans cannabis use and sale.

37 states have approved medical use, and 18 allow recreational use.

States vary in how they handle job protection with relation to cannabis use, with a growing trend to protect jobs.

Employers in every state can continue to make employment decisions based on an employee's current fitness to work.

Two jobs for every one applicant (see slide on low unemployment).

Example: Employer changing pre-employment and random drug testing requirements to exclude cannabis testing.

Issues: Complying with varying state law requirements with respect to off-duty use and screening for cannabis.

Solution: Confirm state requirements and adapt policies accordingly.

Maintain workplace safety policies and procedures that focus on fitness for duty.

Paid Sick Leave

Legal Consideration: State Laws

Facts: United States is one of only three high-income nations without universal paid sick leave.
American women receive 0 weeks of federally mandated paid maternity leave.
16 states (and a number of local governments) have passed laws requiring some form of paid sick leave.
More than 16 states have blocked local governments from creating paid sick leave requirements.

Example: Multi-state employer managing several different sick leave policies across jurisdictions.

Issues: State laws vary in allotments, notice requirements, and record-keeping requirements.

Solution: Confirm state requirements and create policy or policies that broadly cover as many as possible.
Prepare to adapt quickly if needed.
Ensure that payroll company is current and compliant.

Questions?

How have you handled these issues?

What other issues are you facing?

What issue do you anticipate developing in 2023?

大成 DENTONS

Thank you!

Kate Erdel
Partner
Indianapolis
+1 317 968 5339
Kate.Erdel@dentons.com

Katie Jackson
Managing Associate
Indianapolis
+1 317 968 5315
Katie.Jackson@dentons.com

Grow | Protect | Operate | Finance