Colorado's New Privacy Law

July 8, 2021

* The information provided in these slides and the accompanying presentation do not constitute legal advice and should not be substituted for such advice.

Agenda

Introduction

Coverage

Consumer Rights & Notice

Enforcement

Takeaway Discussion

sixfifty

Who (and What) is Protected?

- Consumer = Colorado resident acting in an individual context
  - Commercial and business contexts (e.g., employees and job applicants) not covered
- Personal Data = Information linked (or reasonably linkable) to an identified or identifiable individual
- Sensitive data = Race, religion, sexual orientation, citizenship, health, biometrics, or < 13's data
- Exemptions for de-identified or pseudonymous data and "publicly available information"
- Broad definition of "sale" like the CCPA

Exceptions for Some Data

- De-identified Data
  - Can’t be reasonably linked to an individual, PLUS administrative protective steps
- Publicly Available Information
  - Information lawfully made available from government records and information Controller has a reasonable basis to believe a Coloradan has made available to the general public
- Pseudonymous Data*
  - Identifying information kept separate and administrative protective steps
  - * Exempt IF the controller can’t access the info necessary to re-ID the data

Who Has to Comply?

- Any business that intentionally produces or delivers products or services to Colorado residents AND either:
  - Controls or processes personal data or 100k+ Coloradans; or
  - Sells ANY personal data and controls or processes the data of 25k+ Coloradans
- But there are also many carve-outs

Carve-outs

- Status-based exemptions: financial institutions subject to the GLBA; air carriers; and national securities associations
  - But see 6-1-1304(4) re purpose
  - Regulations might clear this up
- Other exemptions apply to specific data regulated by other privacy laws (e.g., HIPAA, FCRA, GLBA, COPPA, FERPA etc.)
- Non-profits are NOT exempt

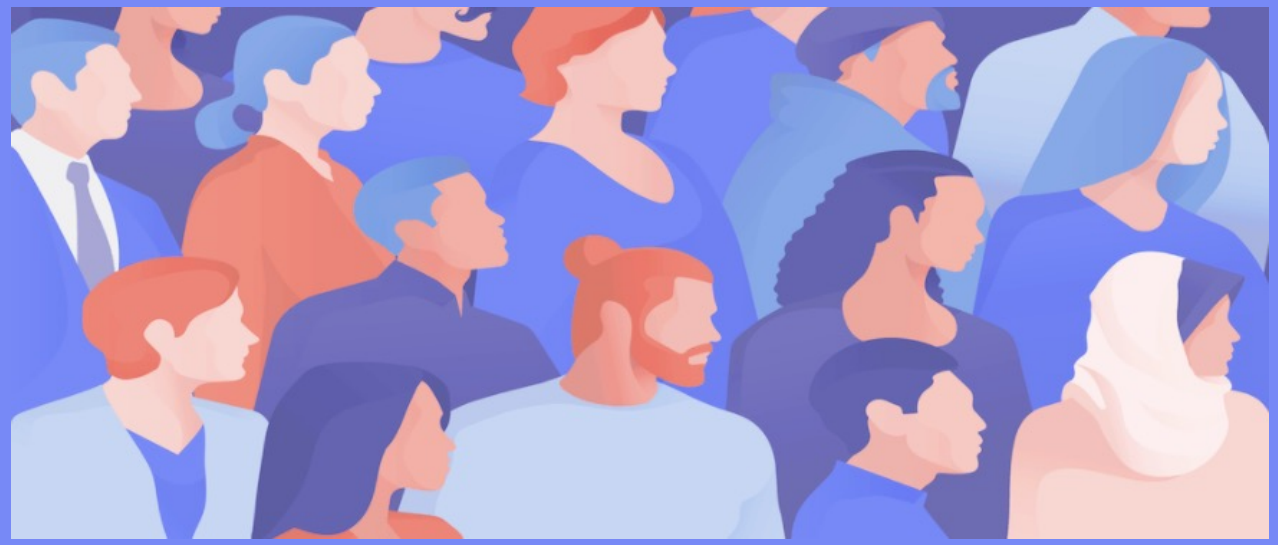
Controller Duties

- Purpose Specification
- Data Minimization
- Avoid Secondary Uses
- Care
- Avoid Unlawful Discrimination
- Date Protection Assessments
  - Processing Sensitive Data
  - Processing for Targeted Advertising

sixfifty

Processor Duties

- Enter into a CPA-compliant processing agreement
- Provide controllers with an opportunity to object before engaging subprocessors
- Assist controllers with CPA obligations
- Assist with responses to data subject requests
    - Use appropriate technical and organizational measure



sixfifty

Consumer Rights

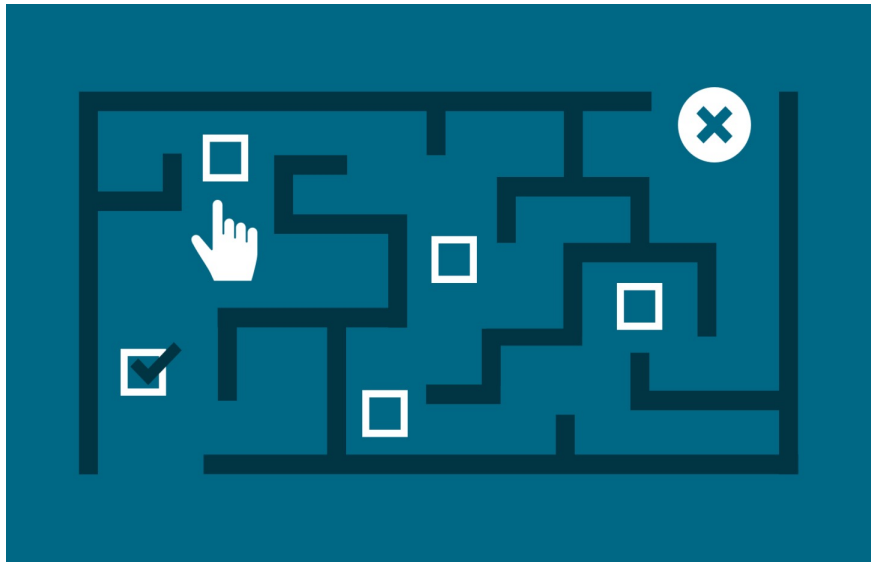
Controllers Must Provide

- Right to Notice
- Right to opt-out of the processing of personal data, including
  - processing for the sale of personal data or
  - profiling in furtherance of decisions that produce legal or similarly significant effects;
- Right of access to confirm whether a controller is processing personal data;
- Right to correct inaccuracies of personal data;
- Right to delete personal data; and
- Right to obtain a portable copy of data.
- NO Private right of action.

sixfifty

Consent

- Like GDPR and other US laws, it requires affirmative act
  - Can’t be part of an agreement that contains unrelated terms
- Processing “sensitive data” requires opt-in consent
- “Dark patterns” negate consent
  - ”A user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice”
  - Quite broad, but consider default options, ease of use, misdirection, all-or-nothing choices, etc.
  - Same definition as CPRA
  - Trend in state (and potential federal) legislation



Cliqz

Additional Operational Items

- Consumers may authorize others to make requests on their behalf
- Controllers must respond within 45 days
  - They can extend by an additional 45 days if reasonably necessary
- A Controller need not fulfill a request if they cannot authenticate the requestor
  - The Controller may request more information for authentication

sixfifty

Enforcement

- Effective July 1, 2023
- Violations are deceptive trade practices
- General consumer protection law determines fines:
  - Up to $20,000 per violation, not to exceed $500,000 in total for any related series of violations; or
  - $10,000 per violation if the Consumer is 60 years old or older, with no cap.
- No private right of action
- 60-day cure provision (until 2025)
- Enforceable by Attorney General AND District Attorneys
  - 22 District Attorney offices in Colorado

Federal Outlook

- State laws' influence
  - Patchwork
  - Seeing trends, setting expectations: right to opt-out, no private right of action, data minimization, DPAs
- FTC rulemaking (!)
  - New chair has been very critical of big tech companies
  - Republican commissioner has announced she now supports this approach

Wikimedia

Key Takeaways

- Broad Definition of “Sale”
- Coverage Rules are More Complex than they Appear
- Enforcement by DAs
- Data Minimization
- DPAs
- Objections to Subprocessors
- Restrictions on Secondary Uses
- Exceptions
  - B2B
  - Employees
  - Specifically Regulated
- Start preparing today!