THANK YOU FOR JOINING

ZOOM MEETING WILL BEGIN SHORTLY

The Consumer Data Protection Act

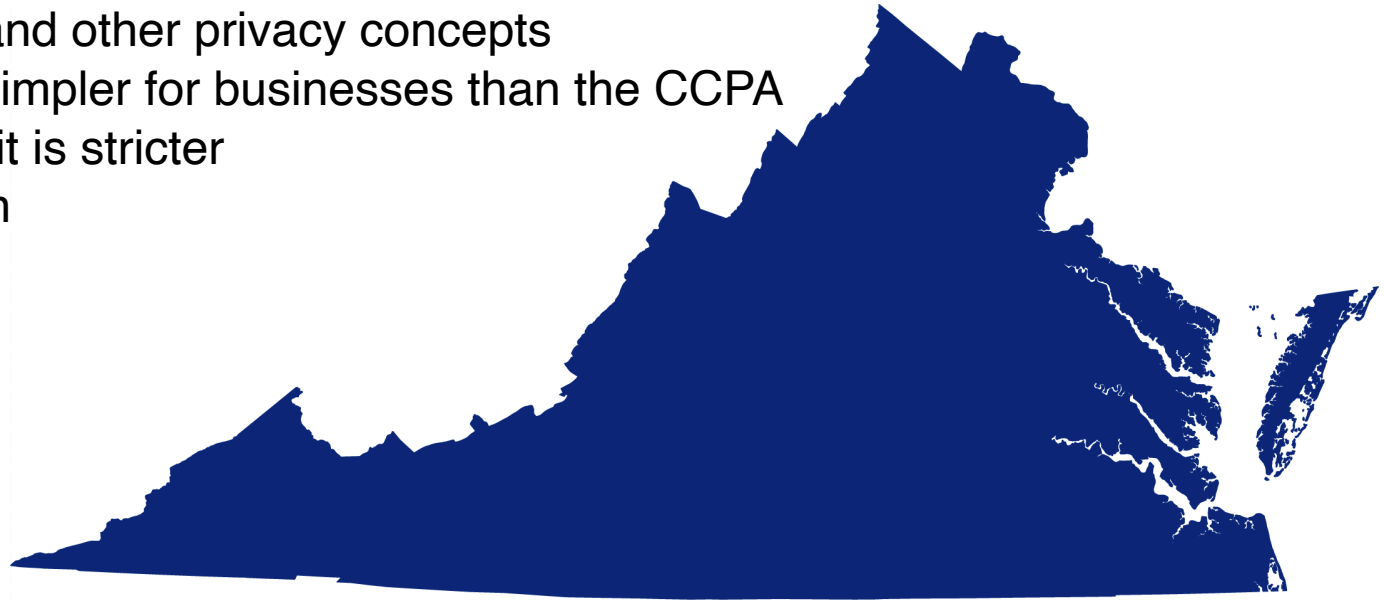
What you need to know about Virginia's new privacy law

Marie Kulbeth,
Austin Smith

*This presentation contains legal information. It is not legal advice. Please consult an attorney for legal advice.

Virginia Consumer Data Protection Act (VCDPA)

- Passed by Virginia General Assembly on Friday, February 19, 2021
- Currently on Governor Northam's desk—he is expected to sign it
- Effective date: January 1, 2023
- Unique mix of CCPA, GDPR, and other privacy concepts
- Compliance is generally a bit simpler for businesses than the CCPA
- However, on a few key issues it is stricter
- Also has a few twists of its own



What Businesses Are Covered?

- Two thresholds for the VCDPA to apply:
  - Controlling or processing the personal data of 100,000 or more Virginia residents in a calendar year
  - Controlling or processing the personal data of 25,000 or more Virginians and deriving over 50% of gross revenue from sale of personal data
- All organizations subject to HIPAA or Gramm–Leach–Bliley exempt
  - Potential drafting error?
- Non-profits and institutes of higher education exempt

What Businesses Are Covered?

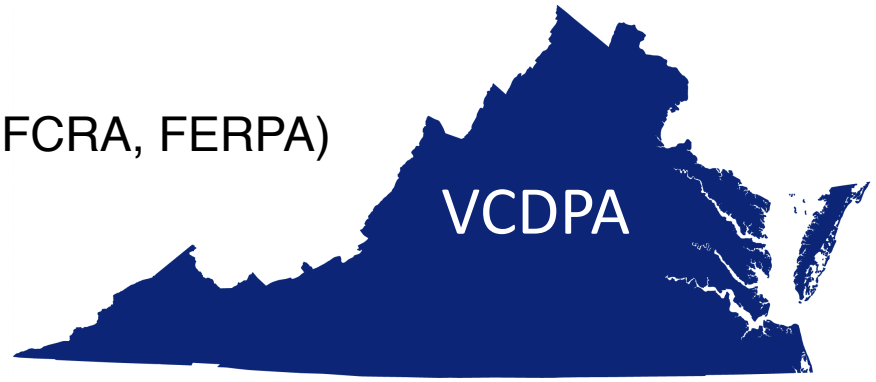
- CCPA Thresholds
  - Nonprofits generally exempt
  - Gov’t agencies exempt
  - Collect, share, or sell CA consumer data AND:
    - Annual gross revenue of >$25 million
    - Personal info of 50,000+ CA consumers, households, or devices
    - Earn >half annual revenue from selling CA consumer PI
- CPRA Thresholds
  - Nonprofits generally exempt
  - Determines means and processing of PI, does business in CA, AND:
    - Annual gross revenue of >$25 million (Jan. 1, year prior)
    - Buy, sell, or share personal info of 100,000+ CA consumers & households
    - Earn >half annual revenue from selling **or sharing** CA consumer PI
    - Joint ventures and partnerships where a member with 40% interest is covered

What Businesses Are Covered?

- GDPR Thresholds
  - Nonprofits included
  - Organizations in the EU
  - Organizations outside the EU if they:
    - Offer goods and services to people in the EU
      - Does the organization cater to EU customers?
      - Does it advertise in the EU?
      - Does it regularly do business in the EU?
    - Monitor the online behavior of people in the EU
      - Does the organization use web tools to track cookies or IP addresses or Europeans who visit the website?
- Exemptions
  - Purely personal or household activity
  - Exempt from some record-keeping requirements if fewer than 250 employees

What Data is Covered?

- Base definition of “personal data” is “any information that is linked or reasonably linkable to an identified or identifiable natural person”
- B2B and employee data is NOT included
- Two subcategories of personal data:
  - Pseudonymous data – fewer obligations
  - Sensitive data – more obligations
- Personal data does **not** include:
  - De-identified data
  - Publicly available information
- Data regulated by federal privacy laws exempt (HIPAA, FCRA, FERPA)



What Data is Covered?

- Base definition of “personal information”
  - Any information that identifies, relates to, or could reasonably be linked *with an individual or household*
- Personal data does **not** include:
  - Aggregate or deidentified consumer info
  - Publicly available information from federal, state, or local gov’t records
    - Professional licenses
    - Public real estate and property records
- *Data* regulated by federal privacy laws exempt (HIPAA, GLBA, Driver’s Privacy Protection Act, FCRA)
- B2B and employment data is generally exempted – notice and security requirements still apply

What Data is Covered?

- Base definition of “personal information”
  - Any information related to an identified or identifiable natural person
  - Subjects are identifiable if they can be ***directly or indirectly*** identified
  - Theoretical identification can be sufficient
  - Must refer to a ***natural*** person ***who is alive***
- Personal data does **not** include:
  - Anonymized data (pseudonymized data IS personal data)
- Publicly available information ***is*** regulated
  - Special rules apply where data is made public by the subject
  - Best to be done on the basis of a law allowing and clearly specifying the data to be published
- No B2B or employment exemptions

Special Categories of Data

- **De-identified data**: take reasonable measures to ensure it cannot be linked to anyone; publicly commit to keep it de-identified; and contractually obligate recipients to comply with the VCDPA
- **Publicly available information**: government records or widely distributed information (e.g., media, or public sharing by consumer)
- **Pseudonymous data**: data that isn't linked to anyone, but could be with other information, maintained separately
- **Sensitive data**: (i) race, ethnicity, religion, health diagnoses, sexual orientation, citizenship, immigration status; (ii) biometric data for identification; (iii) known children's data; and (iv) precise geolocation data (within 1,750 feet, or ~1/3 mile)

Special Categories of Data

- **De-identified data**: (1) harmonized the definition for de-identified health data with HIPAA. (2) information that cannot reasonably identify, relate to, describe, be associated with, or be directly or indirectly linked to a particular consumer where the organization has implemented technical safeguards and business processes prohibiting reidentification and business processes preventing inadvertent release of the info.
- **Publicly available information**: (1) government records or (2) widely distributed information (e.g., media, or public sharing by consumer)
- **Pseudonymous data**: information processed in a ways that renders it no longer attributable to a consumer without using additional information.
- **Sensitive data**: broad definition under CPRA. Personal information that reveals a consumer's government issued ID number, account log-ins or numbers in combination with an access credential, precise geolocation (1/3 mile), race or ethnicity, religious/philosophical belief, union membership, content of mail/messages, genetic data, biometric data (for the purpose of identifying an individual), health data, sex life or sexual orientation data

Special Categories of Data

- **De-identified data**: can include pseudonymized (intermediate) as well as anonymized (complete) data
- **Anonymized data**: the highest, strongest level of deidentification. Once anonymized, data is no longer covered by GDPR.
- **Publicly available information**: still need to notify individuals unless relying on an exception/exemption
- **Pseudonymous data**: data that isn't linked to anyone, but could be with other information, maintained separately. Even if the other information is kept outside your organization, this data is still PI
- **Article 9 Special Categories:** Racial or ethnic origin, Political opinions, Religious or philosophical belief, trade union membership, Genetic data, Biometric data for purpose of identification, Health data, Sex life or sexual orientation

Regulated Uses of Personal Data

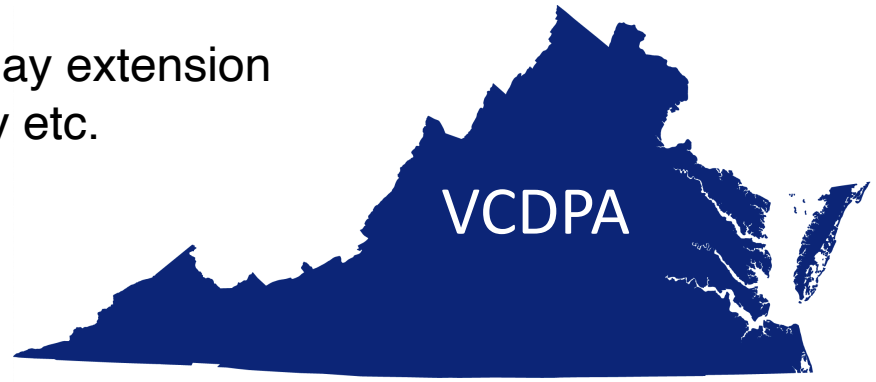
- Sales of personal data: “the exchange of personal data for monetary consideration by the controller to a third party”
- Targeted advertising: showing ads based on personal data obtained from a consumer's activities over time and across nonaffiliated websites or online applications to predict their preferences or interests
    - Does **not** include showing ads based on a consumer’s history on the business’s own website/app, current search terms, or a request for information
- Profiling: automated processing to evaluate, analyze, or predict consumers’ economic situation, health, personal preferences, interests, reliability, behavior, location, or movements
- Data minimization requirement

Regulated Uses of Personal Data

- Consider **everything** regulated under the GDPR
- CCPA: **sale** of personal data, not just for money
- CPRA: **sharing or selling** of personal data
- CPRA: Cross-context behavioral advertising .. Very similar to VCDPA on Targeted advertising
    - Does **not** include showing ads based on a consumer's history on the business's own website/app
    - Service providers are not allowed to engage in CCBA
- **Data minimization** requirement for CDPA and GDPR but not CCPA
- **Profiling**: unlike the VDCPA, profiling may or may not be part of automated decision-making under the CA and EU rules
    - CPRA gives consumers the right to opt out of automated decision-making including profiling
    - GDPR requires a DPIA, notice to consumers, protections for vulnerable groups, lawful basis, allowed to object, collect the minimum amount of data and clear retention policy

Consumer Rights

- Access, correction, deletion, and portability
- Opt-out of sales, targeted advertising, and profiling "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer”
    - Controllers permitted to charge different prices if consumers opt out, or for loyalty programs
- Right to obtain a portable copy of personal data limited to information the consumer provided to the controller
- 45-day deadline for responses to requests; another 45-day extension possible when “reasonably necessary” due to complexity etc.



Consumer Rights

- CCPA: Access (category or Specific), Deletion, Opt-out of Sale, Opt-in Sale (minors)
- CPRA: Access, Deletion, Opt-out of Share or Sell, Limit Use of Sensitive Info, Correction, Opt-in for Share/Sell (minors), Right to Object to Automated Decision Making & Profiling, Some Limited Data Portability
- Portable, machine-readable format
- 45-day responses, 45-day extension possible (15 days for optouts)
- CCPA/CPRA: Opt-In Loyalty and other Incentive Programs are allowed, but the value of the data to the organization must be reasonably related to the value of the incentive/benefit to the customer. CPRA requires a 12-month waiting period before asking a consumer to opt-in after they refuse

Consumer Rights

- GDPR:
  - Be informed
  - Access
  - Rectification
  - Erasure
  - Restrict Processing
  - Data Portability
  - To Object
- One-month responses, from verification, extension to 3 months possible
- Incentives and loyalty programs are allowed, but privacy by design and data minimization principles should be applied

Controller Obligations: Notice

Controllers must provide a privacy notice which includes:

1. Categories of personal data processed;
2. Purposes of processing;
3. How to exercise consumer rights;
4. Categories of personal data shared;
5. Categories of third parties personal data is shared with; and
6. “Clear and conspicuous” disclosure of any sales or targeted advertising [or profiling?]

Controller Obligations: Handling Consumer Requests

- Privacy notice must outline “one or more secure and reliable means” for consumers to submit rights requests, taking into account:
  - How consumers normally interact with the controller;
  - The need for secure and reliable communication of requests; and
  - The ability to authenticate the identity of the consumer
- Controllers must explain how consumers can appeal a decision regarding their request
  - This must be similar to submitting initial request
  - 60-day deadline to respond to appeal
  - Must provide link to contact AG if appeal denied

Controller Obligations: Opt-in for Processing Sensitive Data

- Controllers cannot process sensitive data without consent of the consumer
  - Sensitive data = protected classes, biometric data, children's data, precise geolocation data
- Consent means "a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data"
- For children's sensitive data, must comply with COPPA
  - A child is anyone under 13

Controller Obligations: Data Protection Assessments

- Controllers must conduct data protection impact assessments when (i) processing personal data for targeted advertising; (ii) selling personal data; (iii) profiling consumers in a way that presents a reasonably foreseeable risk of negative impact on consumers; (iv) processing sensitive data; or (v) processing involves “a heightened risk of harm to consumers”
- Assessments must weigh benefits to controller, consumer, and public against risk to consumer, as mitigated by safeguards
- Can re-use assessments done to comply with other jurisdictions
- Don’t need to make them public, but AG can get access to them (not subject to FOIA requests, though)

Enforcement

- No private right of action
- AG enforcement only: injunctions and fines
- Fines up to $7,500 per violation (plus attorney fees)
- 30-day cure period
- Money collected goes into Consumer Privacy Fund to support AG enforcement efforts

Enforcement

- Limited private right of action for higher of
  - $100-750 per consumer per incident or
  - Actual damages
- Fines up to $2,500 per unintentional and $7,500 per intentional violation
- Fines triple for violations regarding children's data under CPRA
- AG/CPPA Enforcement: rulemaking, fines, audits, subpoena power, cease and desist orders

Enforcement

- Private right to seek compensation for material and non-material damage
- Tier 1: Higher of 10 million euro or 2% worldwide revenue
- Tier 2: Higher of 20 million euro or 4% worldwide revenue
- Supervisory authorities can monitor compliances, demand information, review certifications, access premises of controller or processor, order companies to comply with DSARs, issue processing limitations or bans, suspend cross-border data flows, receive individual complaints**, issue fines & injunctions**

Contact SixFifty
Non-Customers: sales@sixfifty.com
Customers: support@sixfifty.com