



Roadmap

- 1. Takeaways
- 2. Quick Recap of CPA
- 3. Consumer Requests
- 4. Universal Opt-Out Mechanism
- 5. Privacy Notices
- 6. Other Processing Requirements

- 7. Loyalty Programs
- 8. Sensitive Data
- 9. Consent
- 10. UI Design, Choice Architecture, and Dark Patterns
- 11. Data Protection Assessments
- 12. Profiling

HUSCH BLACKWELL

Takeaways

© 2023 Husch Blackwell LLP



Takeaways

- 1. Rules effective July 1, 2023 (same date as statute)
- 2. Extensive changes from draft rules (mostly probusiness)
- Specific attention needs to be spent on requirements for sensitive data inferences, privacy notices, processing purposes, secondary uses, data minimization and retention, data protection assessments, and profiling

HUSCH BLACKWELL

Quick Recap of CPA

© 2023 Husch Blackwell LLP

5



Scope

Controller that conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to Colorado residents



100,000

"controls or processes the personal data of" 100,000 "consumers or more during a calendar year"

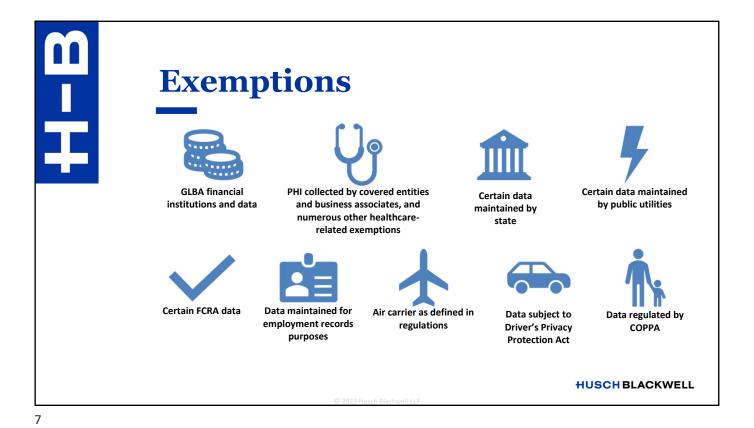
OR

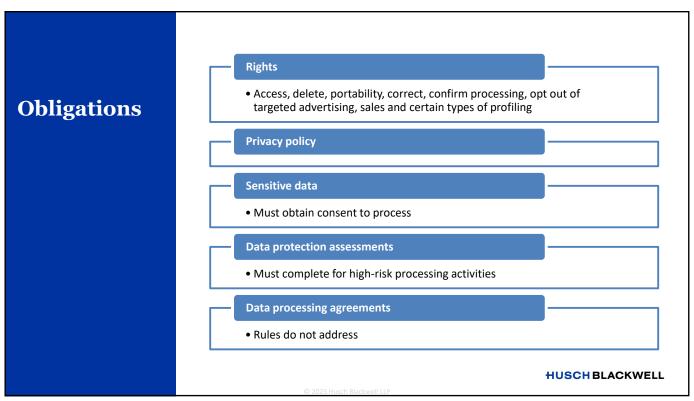
Sell + 25,000

"derives revenue or receives a discount on the price of goods or services from the sale of personal data of" 25,000 "consumers or more"

HUSCH BLACKWELL

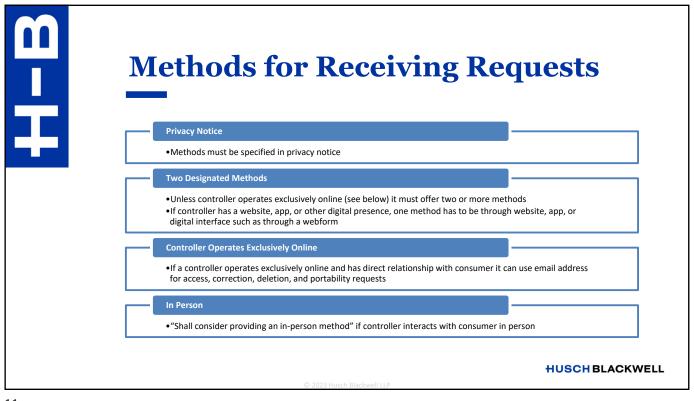
© 2023 Husch Blackwell LLP

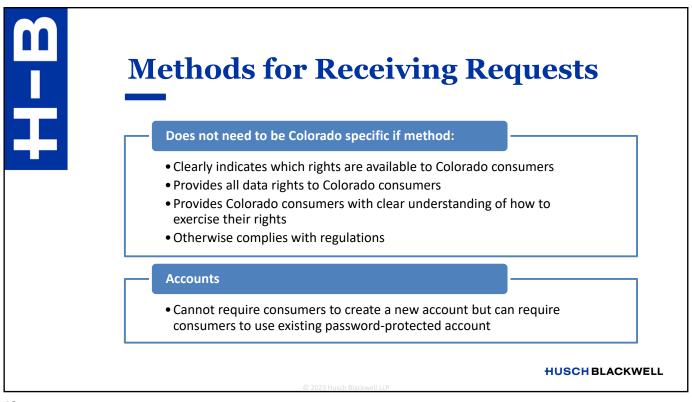






Consumer Requests







Response



Timing

45 days (unchanged from statute)

Requests to opt out must be processed "as soon as feasibly possible and without undue delay"



Denial

If controller denies request, then it must explain basis for denial and provide instructions for how to appeal

HUSCH BLACKWELL

© 2023 Husch Blackw

13

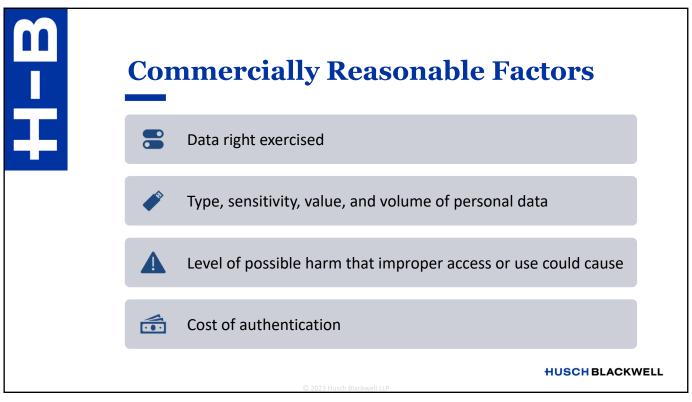


Authentication

Rules are not prescriptive like California's requirements

Need to use "commercially reasonable method" for authentication

HUSCH BLACKWELL





Right to Opt

Sales / Targeted Advertising

 Must provide an opt-out method either directly or through a link, in a clear, conspicuous, and readily accessible location outside privacy notice

Profiling

 Must provide a clear and conspicuous method at or before the time profiling occurs

HUSCH BLACKWELL

17

If link is used it must:

01

Comply with Rule 4.02(B)

 E.g., enable a consumer to submit the request at any time; be easy to execute 02

Take consumer directly to opt-out method

03

Provide clear understanding of purpose

•E.g., "Colorado Opt-Out Rights," "Personal Data Use Opt-Out," "Your Opt-Out Rights," "Your Privacy Choices," "Your Colorado Privacy Choices"

HUSCHBLACKWELL

© 2023 Husch Blackwell LLP

Link Text

Colorado

Any clear and conspicuous method for Consumers to exercise the right to opt out of Processing for the Opt-Out Purposes, provided pursuant to this section, must comply with the requirements of 4 CCR 904-3, Rule 4.02(B). If a link is used, it must take a Consumer directly to the opt-out method and the link text must provide a clear understanding of its purpose, for example "Colorado Opt-Out Rights," "Personal Data Use Opt-Out," "Your Opt-Out Rights," "Your Privacy Choices," or "Your Colorado Privacy Choices."

California

(b) A business that chooses to use an Alternative Opt-out Link shall title the link, "Your Privacy Choices" or "Your California Privacy Choices," and shall include the following opt-out icon adjacent to the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business's internet Homepage(s). The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.



HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

19

Other Rights



Right of Access



Specific Pieces

Must respond with all specific pieces of personal data collected and maintained about consumer, including personal data obtained by processors



Format

Provide data in concise, transparent and easily intelligible form that avoids "incomprehensible internal codes"



Data Breach Protections

Not required to disclose sensitive information such as SSNs and passwords but need to explain that controller has collected that information

HUSCH BLACKWELL

21

Right to Correction

Process

- Must correct personal data in existing systems, except archive or backup systems, and instruct processors to make necessary corrections in their systems
- •Controller can delay compliance for personal data stored on archived or backup systems until they are restored or is next accessed or used

Account Settings

• Can direct consumers to account settings to make corrections under certain circumstances

Standard

- •Controller can require consumers to provide documentation
- •Controller can decide not to act if it determines that contested personal data is more likely than not accurate

HUSCHBLACKWELL



Right to Deletion

Controller must

- Permanently and completely erase personal data or deidentify it
- Notify processors to delete personal data

Archive/Backup Systems

 May delay compliance until system is restored to an active system or is next accessed or used

HUSCH BLACKWELL

23

Universal Opt-Out Mechanism

Universal Opt-Out Mechanism (UOOM)

Purpose

 Consumers can automatically exercise right to opt out of targeted advertising or sale of personal data through UOOM (but not right to opt-out of profiling)

Public List of UOOMs

- No later than January 1, 2024, the Office will maintain a public list of UOOMs that it has recognized
- Controllers have 6 months to recognize UOOM added to the list

Processing of Request

 Controller shall treat UOOM as valid opt out request for browser or device and, if known, for the consumer

HUSCH BLACKWELL

25

Universal Opt-Out Mechanism (UOOM)

Notice

 Controller is permitted, but not required, to display that it has recognized opt-out signals such as by displaying on its website "Opt-Out Preference Signal Honored"

Consent

- Controller may enable consumer to consent to processing for which consumer has opted out so long as request for consent complies with CPA and rules
- If consumer used UOOM to opt out, then controller cannot interpret later absence of UOOM as consent to opt back in

HUSCH BLACKWELL

© 2023 Husch Blackwell LLF

UOOMs and Cookie Banners

"A Consumer opts out of the use of Personal Data for Sale or Targeted Advertising using a Universal Opt-Out Mechanism. The Consumer visits the website of a fashion retailer that routinely shares Consumer Personal Data for Targeted Advertising. The fashion retailer must obtain the Consumer's consent because the Consumer has already opted out of Processing for that purpose. The fashion retailer's website displays a pop-up banner seeking Consent to share the Consumer's Personal Data for Targeted Advertising. This is not a valid request for Consumer Consent because the request is made through a pop-up banner that degrades or obstructs the Consumer's experience on the Controller's web page or application."

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

27

UOOMs and Cookie Banners

"A Consumer opts out of the use of Personal Data for Sale or Targeted Advertising using a Universal Opt-Out Mechanism. The Consumer visits a fashion retailer's website. The fashion retailer's homepage contains a message at the top of the webpage that displays the Consumer's opt-out status, stating, "you have opted out of targeted advertising" next to a link that states "Opt-in to Data Use". The linked webpage also meets all requirements of 4 CCR 904-3, Rules 7.03 and 7.04. Consent pursuant to this request is valid."

HUSCH BLACKWELL



General Notice Requirements

Understandable

Must be "understandable and accessible to a Controller's target audiences"

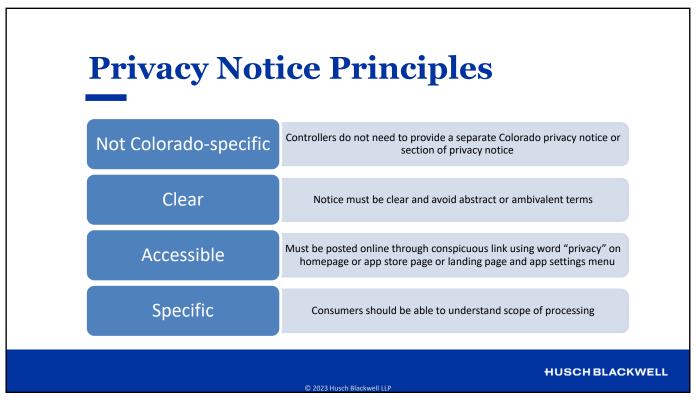
Accessibility

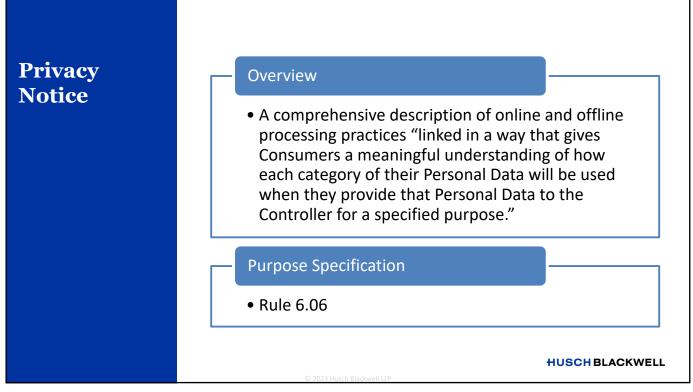
Must comply with Web Content Accessibility Guidelines

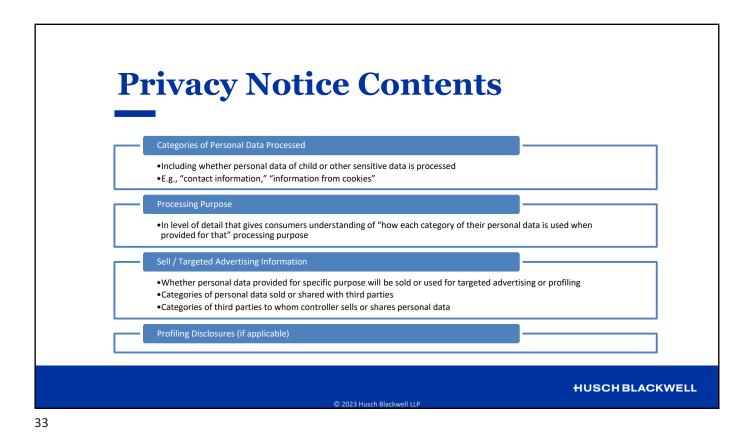
Languages

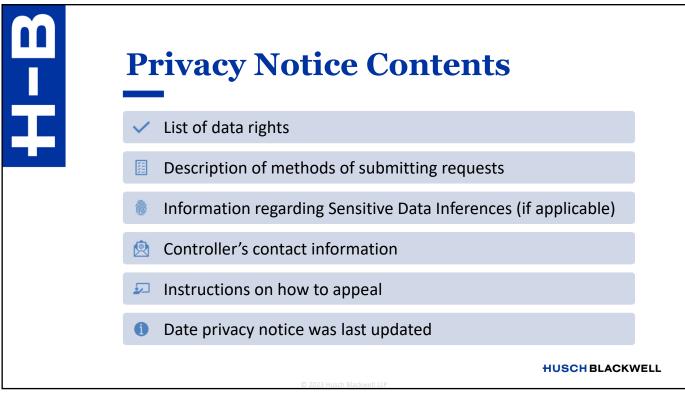
Must be available in languages in which Controller conducts business

Must be readable on all devices, including on smaller screens and mobile apps









Changes to Privacy Notice

Notice of Material Changes

 Must notify consumers of "material changes" to privacy notice

Types of Changes

• Includes changes to (1) categories of personal data processed, (2) processing purposes, (3) controller's identity, (4) act of sharing personal data with third parties, (5) categories of the third parties personal data is shared with, and (6) methods for submitting data rights requests

HUSCH BLACKWELL

35

Other Data Processing Requirements



Purpose Specification



Controllers must specify the "express purpose" for which personal data is collected and processed in both external disclosures to consumers and internal documentation



Must be described in "level of detail that gives Consumers a meaningful understanding of how each category of their Personal Data is used when provided for that Processing purpose"



If data is processed for multiple purposes, controller must specify each

HUSCH BLACKWELL

37



Secondary Use

Consent

 Must obtain consumer consent for processing personal data for purposes "not reasonably necessary to or compatible with specified Processing purpose(s)"

Reasonably Necessary or Compatible

 Controllers should consider 7 factors in making determination

HUSCH BLACKWELL

Data Minimization and Retention

Minimization

 Must determine the minimum personal data that is necessary, adequate, or relevant for each express purpose

Retention

- Personal data kept only for as long as necessary for the express purpose
- Shall set specific time limits for erasure or to conduct a periodic review

HUSCHBLACKWELL

© 2023 Husch Blackwell LLI

39

Loyalty Programs

Definitions

"Bona Fide Loyalty Program"

 A "loyalty, rewards, premium feature, discount, or club card program established for the genuine purpose of providing Bona Fide Loyalty Program Benefits to Consumers that voluntarily participate in that program"

"Bona Fide Loyalty Program Benefit"

 An "offer of superior price, rate, level, quality, or selection of goods or services provided to a Consumer through a Bona Fide Loyalty Program"

HUSCHBLACKWELL

© 2023 Husch Blackwell LL

41



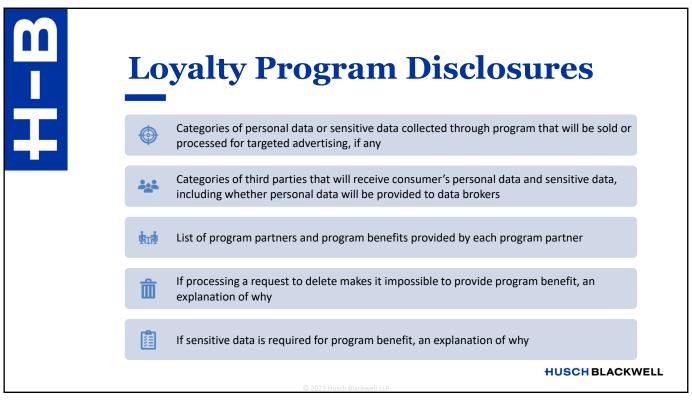
Rules establish structure for:

Interaction between requests to delete / opt out of sale / opt out of targeted advertising and participation in bona fide loyalty program

Consumer refusal to consent to processing of sensitive data necessary for program

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP





Sensitive Data

Consent

 Controllers need consent to process sensitive data and "Sensitive Data Inferences"

Definition of Sensitive Data (§ 6-1-1303(24))

- a)Personal data *revealing* racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status;
- b)Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or
- c)Personal data from a known child.

HUSCH BLACKWELL

45

Sensitive Data Inferences

"Revealing"

• The word "revealing" in definition of sensitive data includes Sensitive Data Inferences

Definition of Sensitive Data Inferences

• Inferences made by a controller based on personal data, alone or in combination with other data, which are used to indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status

HUSCHBLACKWELL

© 2023 Husch Blackwell LLP

Examples

Precise geolocation data showing individual visited a mosque is sensitive data if used to infer religious beliefs

Precise geolocation data showing individual visited a reproductive health clinic is sensitive data if used to infer health condition or sex life

Web browsing data is sensitive data if used to infer an individual's sexual orientation

HUSCH BLACKWELL

47

Can process sensitive data inferences without consent for individuals over 13 only if:

Obvious

• Processing purpose would be obvious to reasonable consumer

Deletion

- Sensitive data inferences are deleted within 24 hours
- Controller also must disclose information regarding sensitive data inferences in privacy notice and data protection assessment

No Transfer

• Sensitive data inferences are not transferred, sold, or shared

Restricted Processing

• Sensitive data inferences are not processed for any purpose other than disclosed express purpose

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP



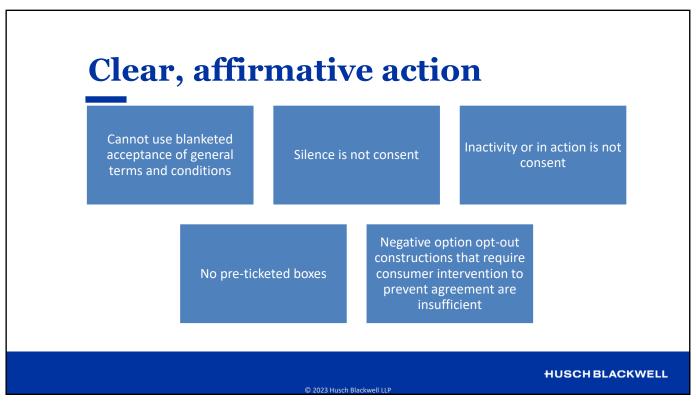
5 Requirements for Valid Consent

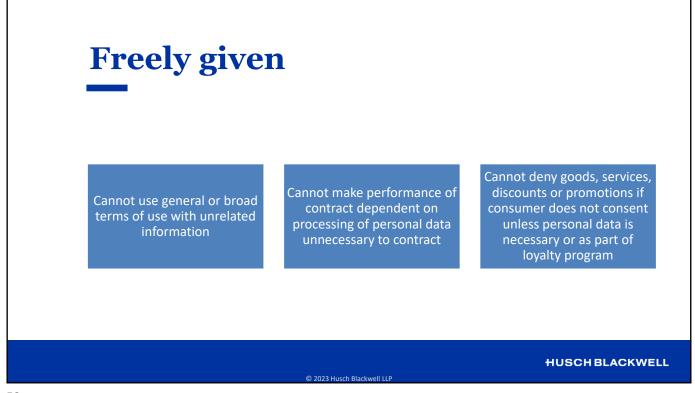
Obtained through clear, affirmative action

Freely given Specific

Informed Reflect consumer's unambiguous agreement

HUSCHBLACKWELL





Specific

Consumers must have ability to separately consent to multiple processing purposes that are not reasonably necessary or compatible

Sale of sensitive data to one party is not necessary or compatible with sale of sensitive data to another party

HUSCHBLACKWELL

© 2023 Husch Blackwell LL

53

Informed

Controller's identity

Reason that consent is required

Processing purpose for which consent is sought

Categories of personal data that the controller shall process

Names of all third parties receiving sensitive data through sale (if any)

Description of right to withdraw consent

HUSCHBLACKWELL

© 2023 Husch Blackwell LLP

Refreshing Consent

24 Months

 If consumer has not interacted with controller in prior 24 months, the controller must refresh consent to process sensitive data and for secondary use purposes if it involves profiling covered by statute's opt out right

Exception

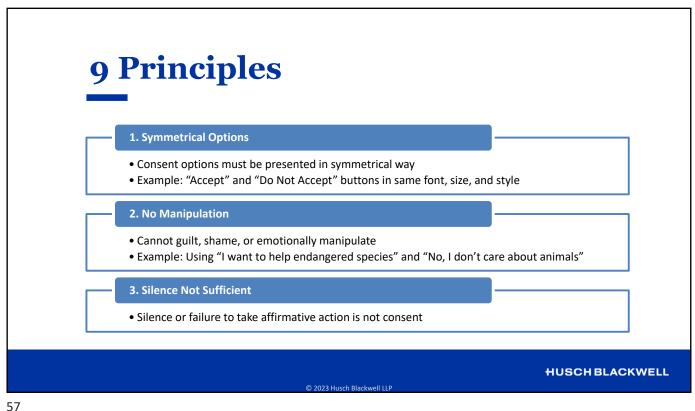
 Controller does not have to refresh consent if consumer has ability to update their opt-out preferences through user-controlled interface

HUSCHBLACKWELL

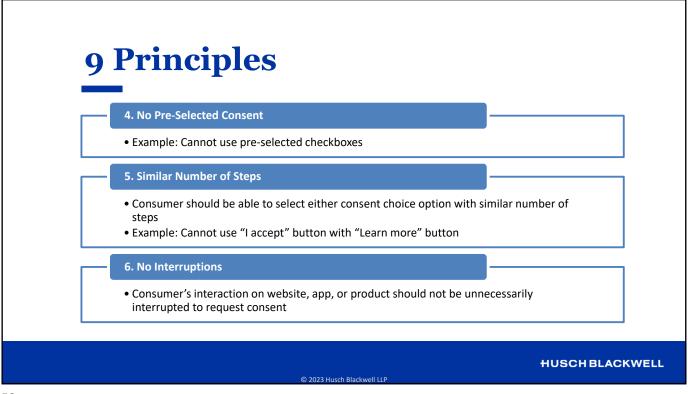
© 2023 Husch Blackwell LL

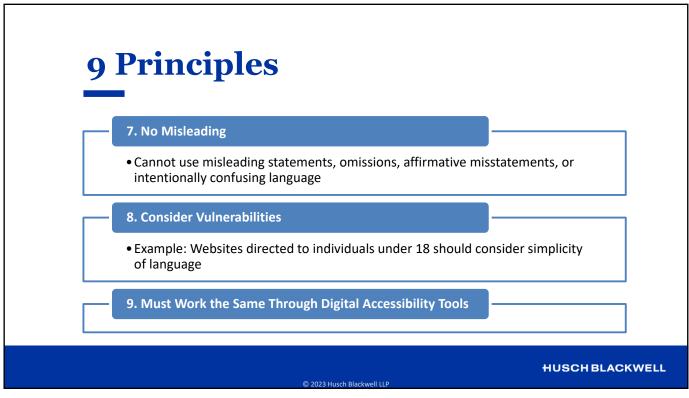
55

UI Design, Choice Architecture, and Dark Patterns

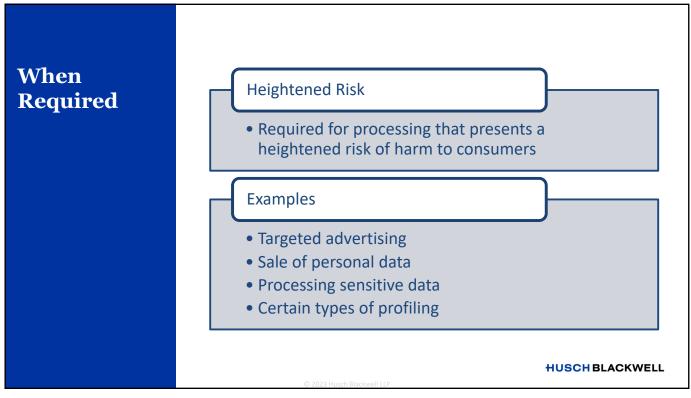


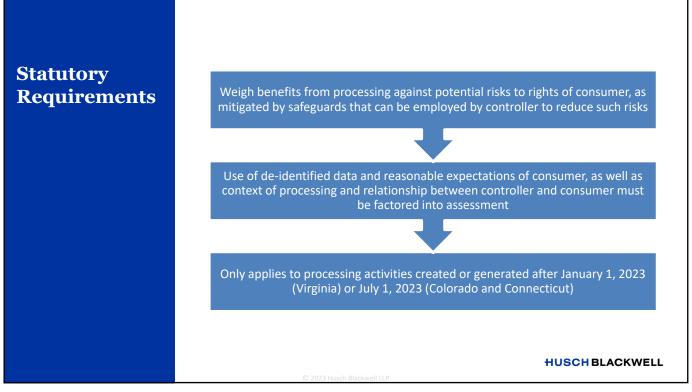
5/

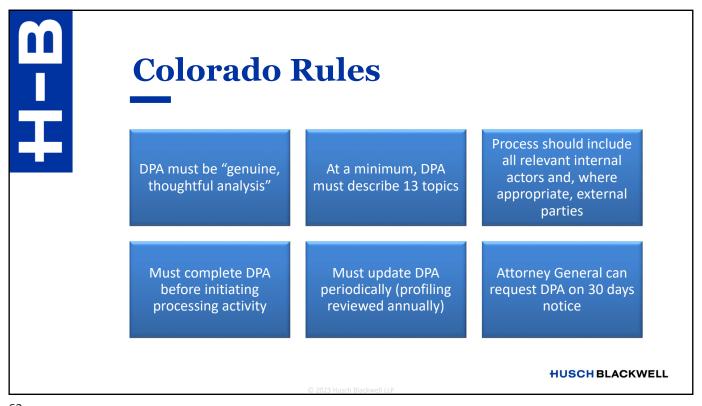


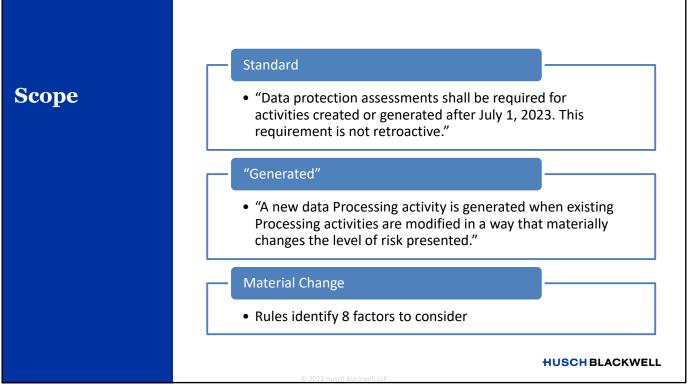


Data Protection Assessments —

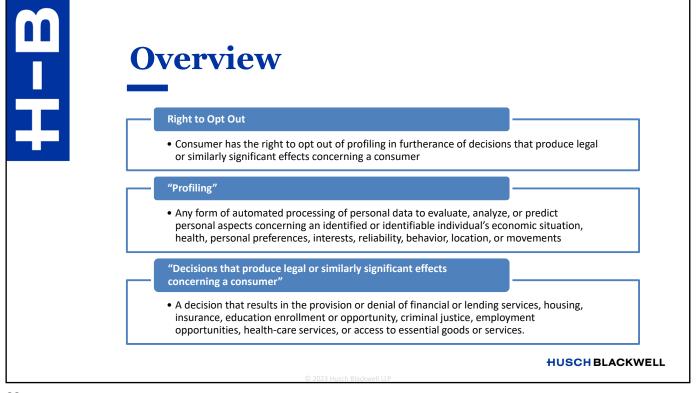




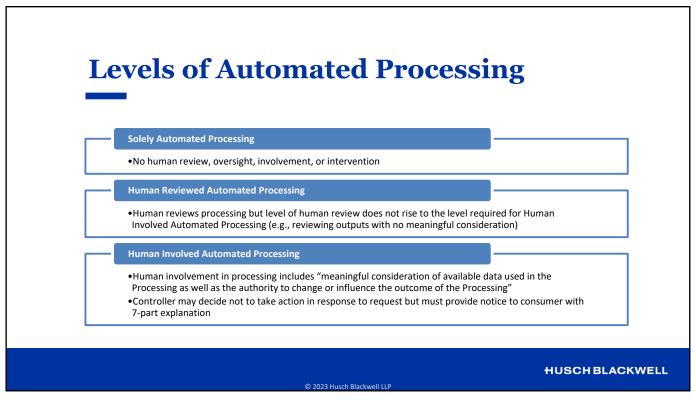








Transparency Notice • Controllers must provide clear, understandable, and transparent information to consumer in privacy notice Notice must include (among other things): • What decision is subject to profiling • Categories of personal data at issue • Explanation of logic used • How profiling is relevant to ultimate decision • If system has been evaluated for accuracy, fairness, or bias



Data Protection Assessments

Controllers must conduct profiling data protection assessments if profiling presents a reasonably foreseeable risk of:

- Unfair or deceptive treatment of, or unlawful disparate impact on consumers
- Financial or physical injury to consumers
- A physical or other intrusion upon the solitude or seclusion, or private affairs or concerns of consumers if the intrusion would be offensive to a reasonable person
- Other substantial injury to consumers

Profiling data protection assessments must:

- Include 12 additional topics
- Be reviewed and updated annually

HUSCH BLACKWELL

© 2023 Husch Blackwell LLF

69



