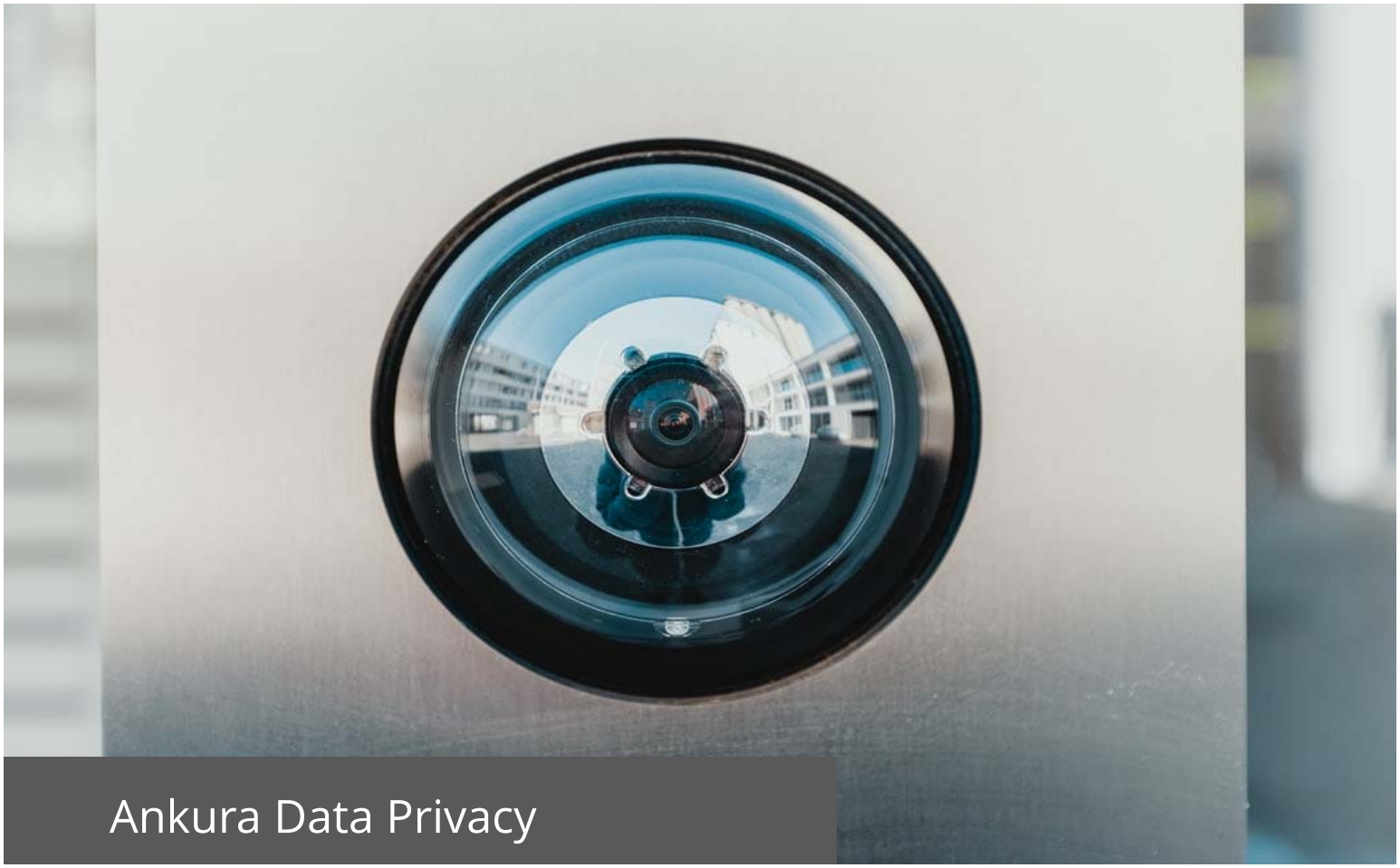


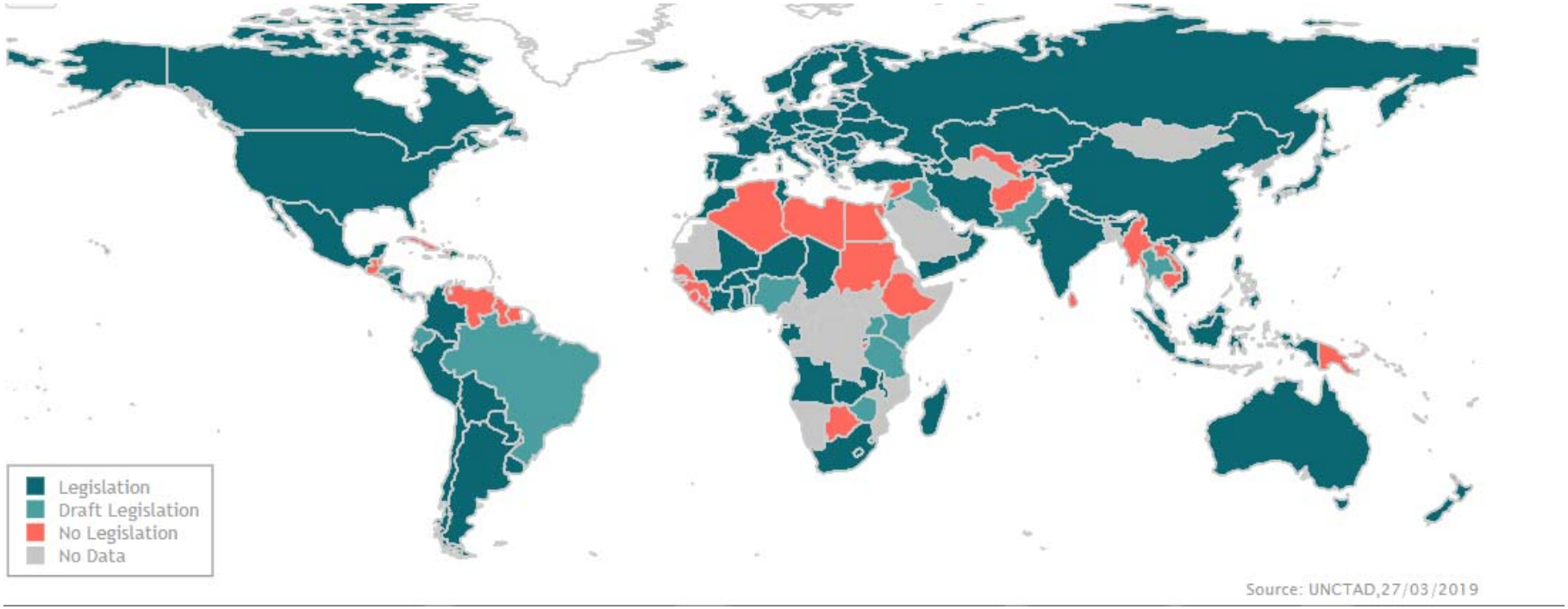
Ankura Data Privacy

ankura

ankura.com

2019

Privacy Landscape



https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Privacy Regulations: Updates & Trends

GDPR Enforcement

Basic technical and organisational security measures remain key to avoiding or mitigating enforcement.

CCPA 2020

Companies should expect core provisions to become effective in July 2020 and should focus on compliance in the coming year.

State Law Trends

The CPPA has inspired proposed privacy laws in 16+ states, which is driving calls for comprehensive federal legislation.

The FTC's Evolving Role

The FTC is leaning into its Consumer Protection mission in advertising & data privacy and the GAO is calling for it to become the primary enforcing agency for internet privacy.

Europe: General Data Protection Regulation Enforcement

UK - Marriott

£99M
$123M

- Data Breach: Marriot acquired Starwood and discovered Starwood's central reservation database had been hacked
- An internal investigation found that the attacker had been able to access the network since 2014
- The database contained records of up to 500 million customers
- The ICO said that companies need to do due diligence when making a corporate acquisition

UK – British Airways

£183M
$230M

- Data Breach: users of British Airways website were diverted to a fraudulent site
- 380,000 transactions were affected, but apparently did not include passport or travel details
- Poor security lead to compromise of log in, payment card, name and address, and other personal information.
- The fine is 1.5% of BA's 11.6B worldwide turnover last year

France – Google

€50M
$57M

- CNIL fined Google for a lack of transparency, inadequate information, lack of a valid legal basis for processing, and no valid consent
- The information related to personalized ads wasn't sufficiently clear and spread across multiple documents
- Consent boxes were "pre-ticked" and consent is only valid if given for each purpose

Denmark – Taxa 4X35

1.2M DKK
$180,000

- Article 5 violation: purpose limitation, data minimization, and storage limitation
- The company used phone numbers of customers for account numbers; the company even admitted phone numbers were not necessary any numerical ID would suffice.
- Danish DPA found during a random audit that Taxa shouldn't have been using Phone numbers in this way, and they had over 9m unnecessary personal records.

State Comprehensive-Privacy Law Comparison

State	Legislative Process	Statute/Bill (Hyperlinks)	Common Name	To Access to Collected	To Access to Shared	To Rectification	To Deletion	To Restriction	To Portability	To Opt-Out	Against Solely Automated Decision Making	Private Right of Action	Strict Age-based Opt-In	Notice/Transparency Requirement	Data Breach Notification	Risk Assessment	Prohibition on Discrimination	Purpose Limitation	Processing Limitation	Fiduciary Duty
California		**Ca. Civ. Code §§ 1798.100 - .199**	**California Consumer Privacy Act**	**x**	**x**		**x**		**x**	**x**		**s**	**16**	**x**			**x**			
~~*Connecticut*~~		~~*SB 1108/HB 1108*~~																		
Hawaii		*SB 418*[I]		*x*	*x*		*x*		*x*	*x*			*16*	*x*	*x*		*x*			
~~*Hawaii*~~		~~*HCR 225*~~																		
Illinois		*HB 3358*	*Data Transparency and Privacy Act*		*x*					*x*				*x*						
~~*Louisiana*~~		~~*HB 249*~~																		
Maine		**LD 946** [II]	**An Act To Protect the Privacy of Online Consumer Information**					**x**		**in**				**x**			**x**			
~~*Maryland*~~		~~*SB 613*~~	~~*Online Consumer Protection Act*~~	~~*x*~~	~~*x*~~		~~*x*~~		~~*x*~~	~~*x*~~				~~*x*~~			~~*x*~~			
Massachusetts		*SD 341/S 120*		*x*	*x*		*x*		*x*	*x*		*x*	*18*	*x*			*x*			
Minnesota		*HF 2917/SF 2912*		*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*			*x*		*x*			*x*	
Nevada		**SB 220/Chapter 603A**								**x**				**x**	**x**					
New Jersey		*S2834*			*x*					*x*				*x*			*x*			
~~*New Mexico*~~		~~*SB 176*~~	~~*Consumer Information Privacy Act*~~	~~*x*~~	~~*x*~~		~~*x*~~		~~*x*~~	~~*x*~~		~~*s*~~	~~*18*~~	~~*x*~~			~~*x*~~			
New York		*SB S5642* [III]	*New York Privacy Act*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*		*x*	*x*				*x*	*x*
~~*North Dakota*~~		~~*HB 1485*~~																		
Pennsylvania		*HB 1049*	*Consumer Data Privacy Act*	*x*	*x*		*x*			*x*		*s*	*16*	*x*			*x*			
Rhode Island		*HB 5930/S0234*	*Consumer Privacy Protection Act*	*x*	*x*		*x*		*x*	*x*		*x*	*16*	*x*			*x*			
~~*Texas*~~		~~*HB 4390*~~ [IV]	~~*Texas Privacy Protection Act*~~																	
Washington		*SB 5376*	*Washington Privacy Act*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*			*x*	*x*	*x*				

In Session:
MA, NJ, PA

Introduced
In Committee
Crossed Chamber
Cross Committee
Passed
Signed

Bold - passed law
Italics - proposed bill, not passed
s - private right of action for security violations only
in - opt-in consent requirement

~~Black strikethrough - bill postponed indefinitely~~
~~Purple strikethrough - task force substituted for comprehensive bill~~

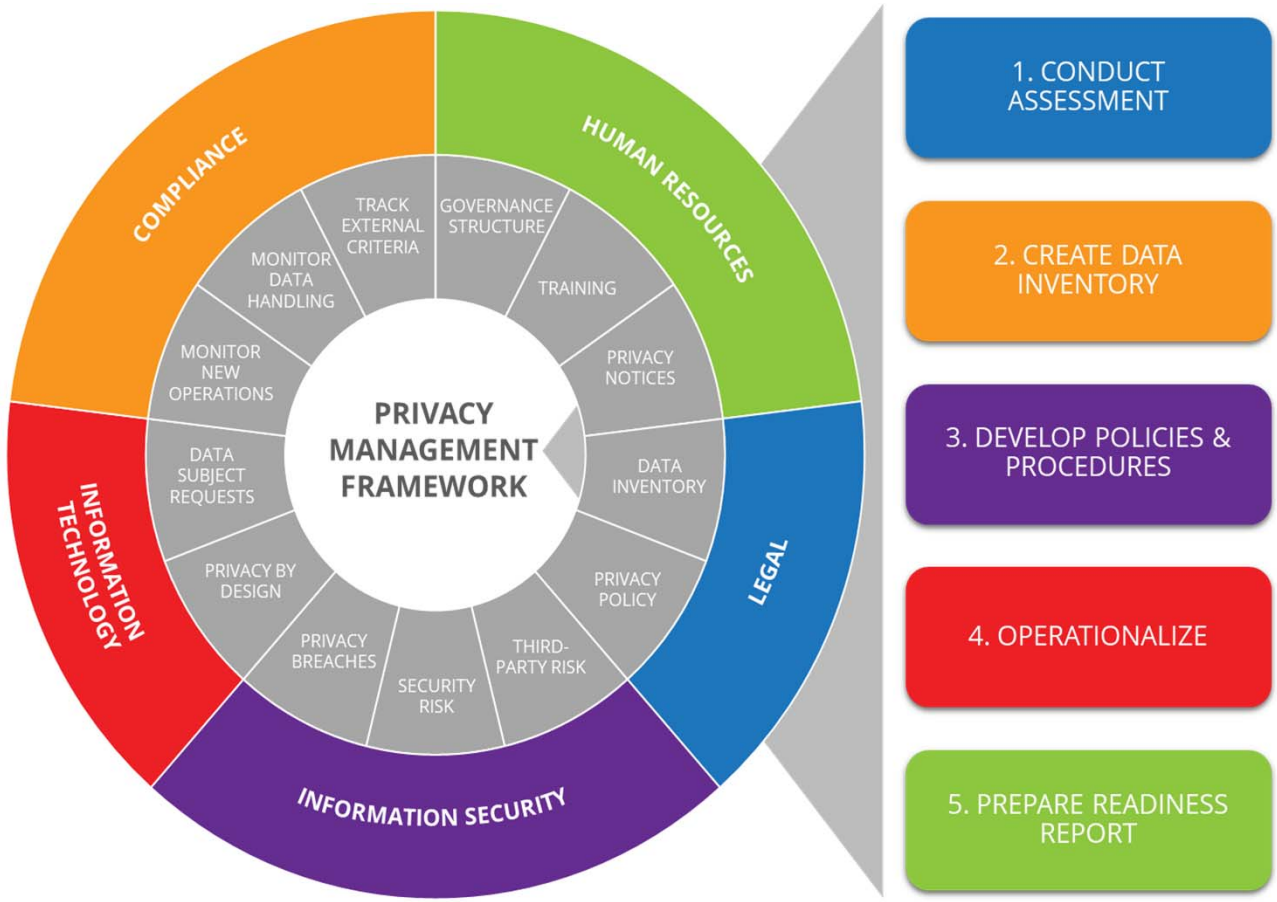
https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/

Five Tips for Success

1	Develop a compliance program	Develop a holistic privacy and security compliance program that can adjust with changing regulations.
2	Put someone in charge	Put someone internal at the company in charge of privacy, whether that be a person or, better yet, a committee.
3	Take a risk-based approach	Assess your risk and develop your program to match the risk.
4	Create a workplan and timeline	The only way you will ever be successful is if you have a plan and a timeline.
5	Tools are not everything	Automated privacy tools are helpful, but they are only part of what you need to create a full privacy compliance program.

ankura

Five Phased Approach to Privacy Compliance Program



ankura

Sample Tools

Prioritization Strategy: Most important activities

1. Data Inventory
2. External Facing Notice
3. Consumer Rights Requests/Data Subject Access Requests
4. Opt out of Sale
5. Minor's Personal Information
6. Third Party Contracts
7. Information Security

Data Inventory: Exclude

1. Exclude:
    - GLBA
    - HIPAA
    - De-Identified
    - Aggregated
2. De-prioritize (delayed until 1/21/2021):
    - Employee data
    - B2B personal information (personal information of individuals acting on behalf of a business shared in B2B interactions)

Data Inventory: Prioritize

Data Sensitivity – Systems or processes that deal with more sensitive data points (things like SSN, credit card info, etc) should be higher priority than those that don't.

Data Volume – Systems or processes that store or process data for a larger volume of people should be higher priority than those that deal with a smaller volume.

Security – Any processing that may be storing or moving data that is not secured (not encrypted or not protected that could pose a risk of breach).

Type of Processing – Marketing related activities or activities where the consumer may not know what you are doing with their data.

External Facing Privacy Notice: Format

Processing Category	Description	Source	Business Purpose	Categories of Third Parties Disclosed	Reason for Sharing with Third Parties
Biometric information	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	• Directly from covered individuals • Covered individuals' devices • From our Business Partners	• Performing Services	• Service Providers	• Performing Services
Protected classifications	Characteristics of protected classifications under California or federal law, like race, religion, gender, national origin, or sexual orientation.	• Directly from covered individuals	• Debugging to repair errors	• Service Providers • External Agencies	• Performing Services

ankura

External Facing Privacy Notice: Potential language

-good faith understanding of the law and our practices as of the date posted

-CCPA's implementing regulations are not yet final and there remain differing interpretations of the law

-may update or modify:

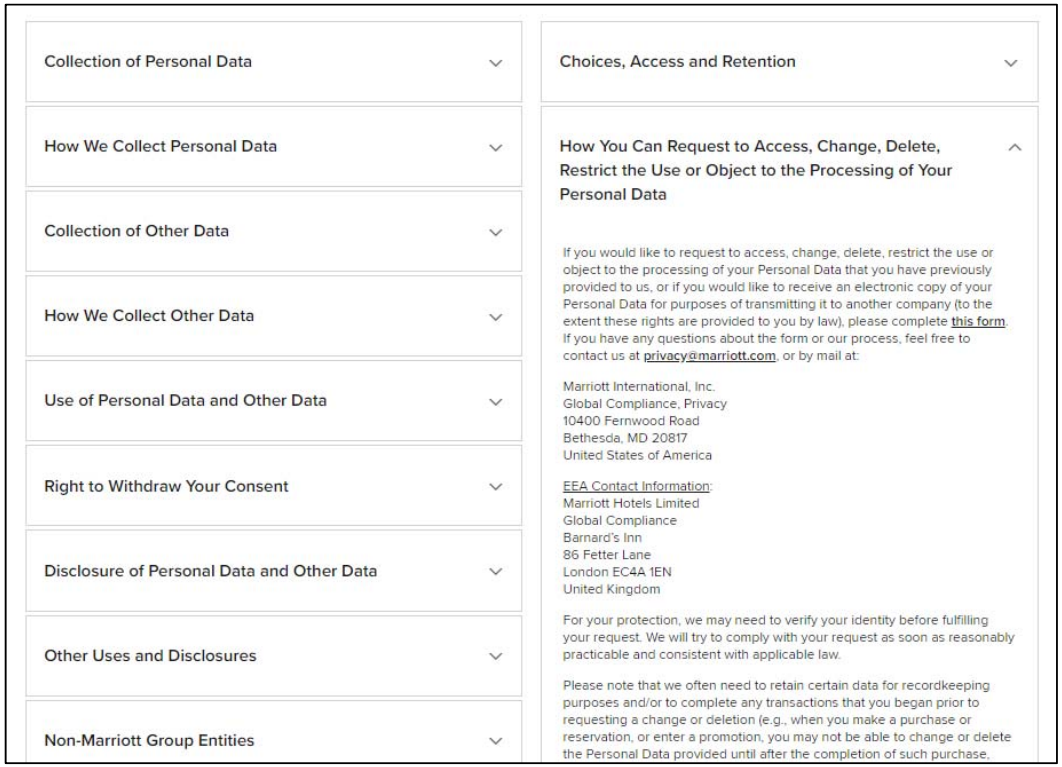
- **information in this notice**
- **our data practices**
- **our understanding of your rights**
- **our methods for responding to your requests**

-we continue to develop our compliance program to reflect the development of the law and our understanding of how it relates to our data practices

ankura

Consumer Rights Request (CRR) / Data Subject Access Request (DSAR)

What are other companies doing?



- Collection of Personal Data
- How We Collect Personal Data
- Collection of Other Data
- How We Collect Other Data
- Use of Personal Data and Other Data
- Right to Withdraw Your Consent
- Disclosure of Personal Data and Other Data
- Other Uses and Disclosures
- Non-Marriott Group Entities
- Choices, Access and Retention
- **How You Can Request to Access, Change, Delete, Restrict the Use or Object to the Processing of Your Personal Data**

If you would like to request to access, change, delete, restrict the use or object to the processing of your Personal Data that you have previously provided to us, or if you would like to receive an electronic copy of your Personal Data for purposes of transmitting it to another company (to the extent these rights are provided to you by law), please complete this form. If you have any questions about the form or our process, feel free to contact us at privacy@marriott.com, or by mail at:

Marriott International, Inc.
Global Compliance, Privacy
10400 Fernwood Road
Bethesda, MD 20817
United States of America

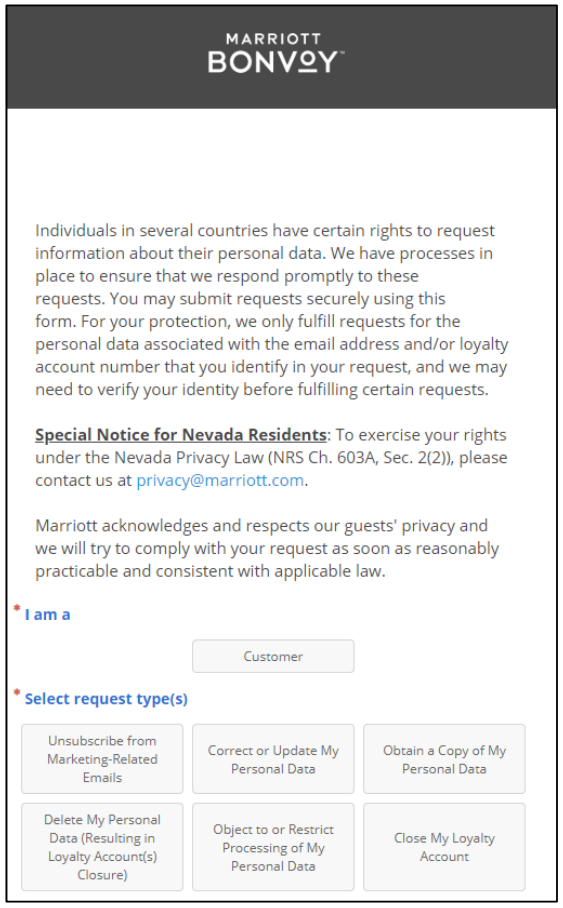
EEA Contact Information:
Marriott Hotels Limited
Global Compliance
Barnard's Inn
86 Fetter Lane
London EC4A 1EN
United Kingdom

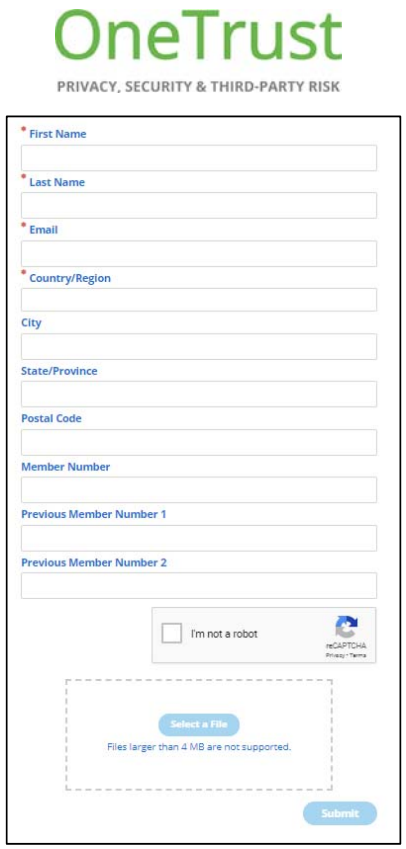
For your protection, we may need to verify your identity before fulfilling your request. We will try to comply with your request as soon as reasonably practicable and consistent with applicable law.

Please note that we often need to retain certain data for recordkeeping purposes and/or to complete any transactions that you began prior to requesting a change or deletion (e.g., when you make a purchase or reservation, or enter a promotion, you may not be able to change or delete the Personal Data provided until after the completion of such purchase.

Example Source:
https://www.marriott.com/about/privacy.mi

Consumer Rights Request (CRR) / Data Subject Access Request (DSAR)



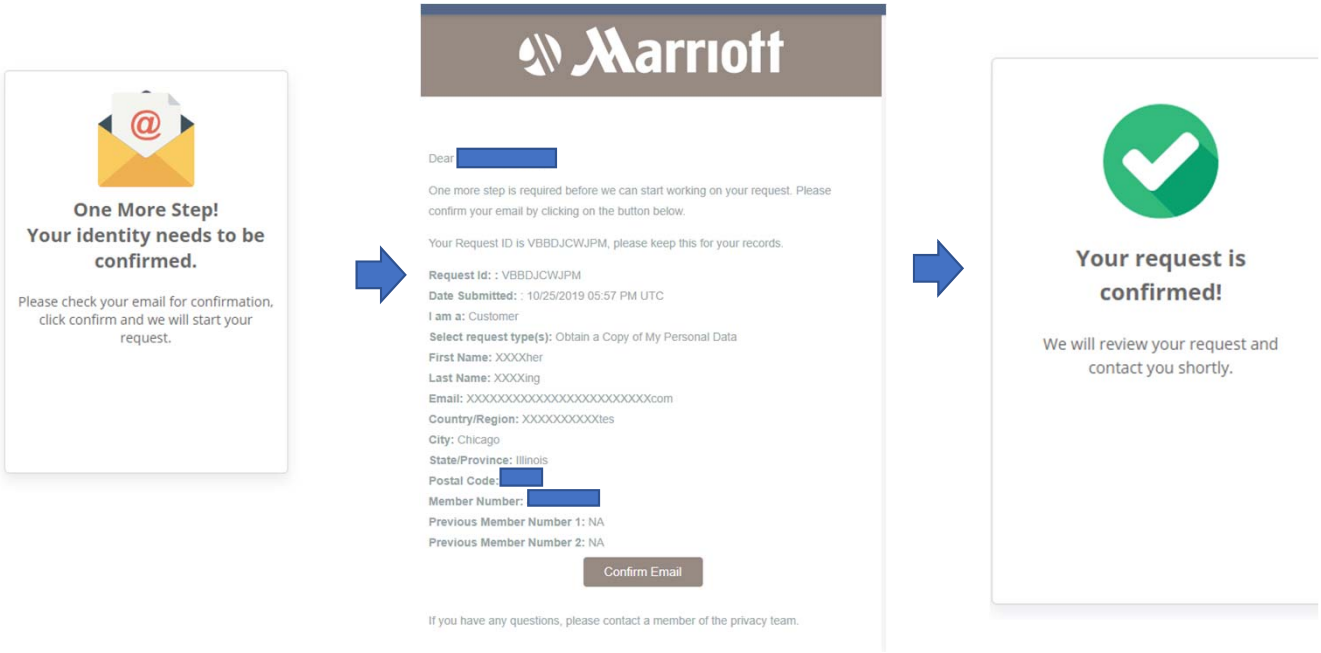


- Include Data Subject Group types as options.
- Make Request Types multiple choice instead of free-form textboxes.

Example Source:
https://privacyportal-cdn.onetrust.com/dsarwebform/0894cd2c-85ba-4d0b-8ec1-e18f3735e0e0/e4eef8ab-3071-4679-a374-5847fbe290de.html

Consumer Rights Request (CRR) / Data Subject Access Request (DSAR)

- Requires email address for identity verification. **Requestor must click on verification link sent by email.**



Example Source:
https://privacyportal-cdn.onetrust.com/dsarwebform/0894cd2c-85ba-4d0b-8ec1-e18f3735e0e0/e4eef8ab-3071-4679-a374-5847fbe290de.html

Opt-Out of Sale of Data

1. Make sure you understand definition of sale under CCPA and engage counsel to confirm instances where you sell data.
2. Consider using a tool to implement a “do not sell” button on your website.

ankura

Minor's Data: Opt-In

1. Use data inventory and understand what information you are collecting and what processing activities are truly targeting minors.
2. Consider language to make it clear that you don't accept minors data where possible.
3. If you collect minors data, implement a tracking tool for consent.
    - Between ages 13 and 16, track minor's consent.
    - Under age 13, track parental consent.

Current Contracts: Risk-based approach

1. Data Volume
2. Data Sensitivity

New or Renewal Contracts: All

Information Security: CIS Top 20

ARLINGTON, Va., Feb. 22, 2016 /PRNewswire/ -- A report released this week by California Attorney General Kamala Harris concludes that the CIS Critical Security Controls represent "a minimum level of information security that all organizations that collect or maintain personal information should meet." Further, the report concludes that **failing to implement the Controls "constitutes a lack of reasonable security."** The report refers to a 2004 California information security law requiring businesses that collect personal information to use "reasonable security practices and procedures."