

NMHC Data Privacy Standards & Compliance Summit



Policy Update: How We Got Here

Kevin Donnelly, Vice President, Government Affairs, NMHC

Julianne Goodfellow, Senior Director, Government Affairs, NMHC

Kaylee Cox Bankston, Counsel, Manatt, Phelps & Phillips, LLP



Coming Soon: Stronger Consumer Data Protections

Kaylee Cox Bankston

Manatt, Phelps & Phillips, LLP



Setting the Stage for a New Privacy Framework

- Historical U.S. State and Federal Activity
 - Breach Notification
 - Data Security
 - Data Privacy
- EU General Data Protection Regulation
- CCPA...and more states to come



Emerging Standards and Common Themes

- Extraterritorial Reach
- Expanded Definition of Personal Information
- Transparency and Notice
- Data Subject Rights
- Data Security and Breach Notification
- Third-Party Oversight
- Governance and Risk Assessments
- Liability



California Consumer Privacy Act (CCPA)

- **The nation's broadest and most comprehensive consumer privacy and data protection legislation**
- Born out of a tumultuous political process, including a popular statewide initiative
- Similar to the GDPR, it is intended to apply across industry sectors and strengthens the rights of individuals, giving California consumers more control over their data
- Applicability:
 - Must be a for-profit entity,
 - Must process data of California residents, and
 - One of the following must be true:
 - Annual revenues > \$25 million;
 - Obtains Personal Information of 50,000 or more California residents annually; or
 - Derives 50%+ annual revenue from selling California residents' Personal Information



CCPA - Personal Information

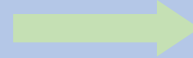
- What data is regulated?
 - Any data identifying a single person or household, or reasonably capable of doing so if combined with additional data.
 - “Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household...

Name	Mail address	Phone number	Email address	IP address	Account info
SSN	Driver's license	Passport number or other ID	Biometrics	Geolocation	Protected classifications
Financial information	Medical information	Health insurance information	Commercial information	Education	Employment
Internet activity, browsing, search	Physical characteristics	Visual	Audio	Thermal	Olfactory



California Consumer Privacy Act (cont'd)

Notice and Consent



Inalienable Rights

Primary Rights

Right to
Access Data

Right to Opt Out
of Data Sales

Right to
Deletion of Data

Private Right of Action
for Data Breaches

Associated Rights

Respond to Requests

Service Provider Obligations

Right of Portability

Penalties for Noncompliance

Nondiscrimination

Enhanced
Privacy Notices



California Consumer Privacy Act (cont'd)

- Enforced by the California Attorney General

- 30-day right to cure
- Impact of CCPA's 12-month "look back" requirement

- Penalties for Noncompliance

- Up to \$2,500 per violation under unfair competition law
- Up to \$7,500 per *intentional* violation of CCPA

- Data Breaches

- Enforceable by *private* right of action
- 30-day right to cure
- Greater of \$100–\$750 per incident, per consumer, or actual damages
- Security requirements "appropriate to the nature of the information"
- Alleged data breaches have instant litigation risk



California Consumer Privacy Act (cont'd): Clarifying Amendments Passed

AB 25 Employee Data Exemption*	AB 1355 B2B Exemption* FCRA Exemption Nondiscrimination Data Minimization	AB 874 PI Definition Reasonableness
AB 1202 Data Broker Registration	AB 1146 Vehicle Information Exemption	AB 1546 Method of Contact Exception

*Subject to a one-year Sunset on January 1, 2021



California Consumer Privacy Act (cont'd): Proposed Regulations Released

Notices	<ul style="list-style-type: none">▪ Notice at Collection▪ Notice at Sale▪ Notice of Right to Opt Out of Sale	<ul style="list-style-type: none">▪ Notice of Financial Incentive▪ Notice to Minors▪ Privacy Policy
Consumer Requests	<ul style="list-style-type: none">▪ Methods for Submitting Consumer Requests to Access and Delete▪ Responding to Consumer Requests to Access and Delete	<ul style="list-style-type: none">▪ Requests to Opt Out▪ Verification Process for Consumer Requests
Business Operations	<ul style="list-style-type: none">▪ Nondiscrimination Practices▪ Service Providers▪ Training	<ul style="list-style-type: none">▪ Record Keeping▪ Special Rules for Minors

Regulations Released on October 10 → Public Comments Due by December 6



A Patchwork of Privacy Legislation

- National-level conversations about monetizing data and privacy
- Demand for data protection legislation is growing across the country
- **Prediction:** Will continue to see consumer demand supporting companies taking strong, public approach to data protection



Prospects for a Federal Privacy Law: Proposed Legislation

- Several bills have been introduced with comprehensive privacy legislation to varying degrees but no substantial progress to date
- Bills have focused on a wide variety of issues, including:
 - Pre-emption, disclosure requirements, breach notification, genetic information, social media, opt-in requirements, FTC's role in enforcement, and private right of actions
- A comprehensive bipartisan bill is expected to be released by the end of 2019
 - Senate Commerce Committee: Senators Richard Blumenthal (D-CT), Jerry Moran (R-KS), Brian Schatz (D-HI), Roger Wicker (R-MS), Maria Cantwell (D-WA), and John Thune (R-SD)
- Biggest challenges so far:
 - Pre-emption, scope, and enforcement



Data Privacy Readiness Roundtable

Scott Lashway, Partner, Manatt, Phelps & Phillips, LLP

Kaylee Cox Bankston, Counsel, Manatt, Phelps & Phillips, LLP



Entrata, Inc.

Jamis Gardner, Chief Legal Counsel, Entrata, Inc.



DATA PROTECTION OBLIGATIONS

- ● 11. Data Security - controls related to the confidentiality, availability and integrity of personal data
- ● 12. Breach Notification – identification of and response to data breaches

RECORDS MANAGEMENT OBLIGATIONS

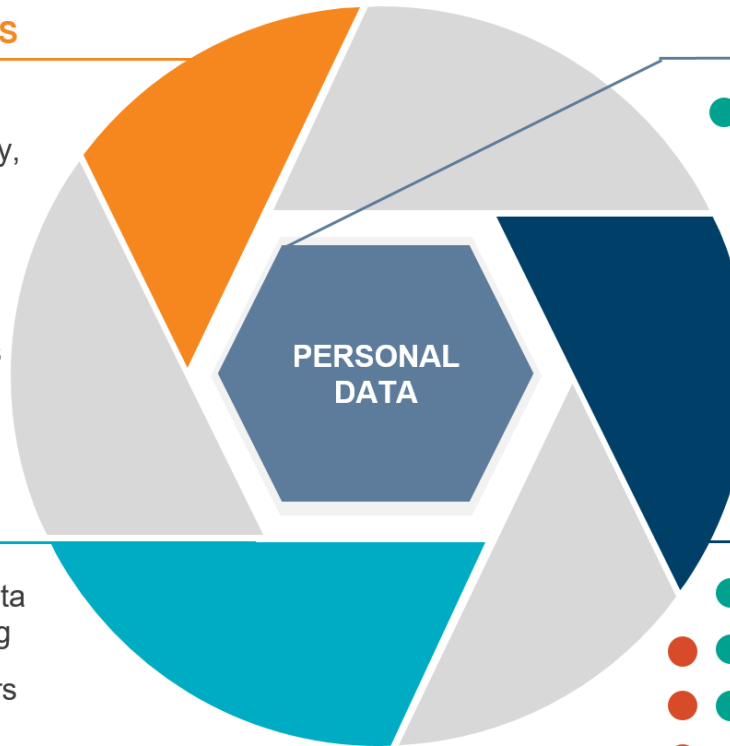
- ● 7. Records of Processing – data inventory and recordkeeping
- 8. Cross-Border Data Transfers
- 9. Third Party Management – contracts and due-diligence
- 10. Privacy by Design & Default – records retention, data minimization, and system design

GOVERNANCE OBLIGATIONS

- 1. Data Protection Officer (DPO)

PRIVACY OBLIGATIONS

- 2. Legal Basis for Processing
- ● 3. Privacy Notice & Disclosures
- ● 4. Consent Management
- ● 5. Individual Privacy Rights
- 6. Privacy Impact Analysis



Privacy Law: ● General Data Protection Regulation (GDPR) ● California Consumer Privacy Act (CCPA) & Civil Code

© 2019 Protiviti – Confidential.



1. Data Protection Officer

Evaluate privacy and data protection governance structure and the need for a Data Protection Officer (DPO).



5. Individual Privacy Rights

Evaluate processes that address the rights of individuals (e.g., access, rectification, erasure, and portability of personal data).



9. Third-Party Management

Evaluate contractual agreements and control validation procedures for third-party vendors with whom personal data is shared.



2. Legal Basis for Processing

Evaluate the legal basis on which personal data is collected and processed.



6. Privacy Impact Analysis

Evaluate data collection and usage practices to determine if a Data Protection Impact Assessment (DPIA) is required



10. Privacy by Design & Default

Evaluate data minimization and retention practices; validate that privacy safeguards are considered prior to new implementations.



3. Privacy Notice & Disclosures

Evaluate external privacy notice and disclosures as well as internal policies and employee training procedures.



7. Records of Processing

Evaluate records of processing activities and data inventories as well as the process to maintain such records.



11. Data Security

Evaluate data security controls employed to help ensure confidentiality, availability and integrity of personal data.



4. Consent Management

Evaluate consent practices, when relying on individual's consent for processing personal data.



8. Cross-Border Data Transfer

Evaluate the legitimate mechanisms for transferring personal data outside of the defined territory.



12. Breach Notification











Evaluate the Incident Response procedures and the breach notification process.



Privacy Law:  General Data Protection Regulation (GDPR)  California Consumer Privacy Act (CCPA) & Civil Code

© 2019 Protiviti – Confidential.



Privacy Right	GDPR	CCPA	
Right to be Informed	Right to be given information about how personal data is being processed and why	Right to be given information about the categories of personal data that is being collected, prior to collection taking place and upon request	
Right to Access	Right to access all personal data in a user-friendly, readable format.	Right to access personal data collected in the last 12 months, delineated between sold and transferred	
Right to Portability	Must export personal data processed in a machine readable file format.	Must export personal data collected in the last 12 months in a machine readable file format	
Right to Correction	Right to correct personal data	Not included with CCPA	
Right to Stop Processing	Right to withdraw consent and stop processing personal data	Right to opt-out of selling personal data only; but there is no requirements to stop collection/processing	
Right to Stop Automated Decision-Making	Right to require a human to make decisions that have a legal effect	Not included with CCPA	
Right to Erasure	Right to erase personal data processed, under certain conditions	Right to erase personal data collected, under certain conditions	
Right to Equal Services & Price	Implicitly required	Explicitly required	
Private Right of Action Damages	No limitation of liability	Liability is limited from \$100 to \$750 per individual per incident	
Regulator Penalties	Limited to 20 million or 4% of global revenue	No limitation - \$7,500 per individual violation	

CCPA Requirements Scope: Not Applicable  Similar Scope  Increased Scope  Reduced Scope 

© 2019 Protiviti – Confidential.



Protiviti & Robert Half Legal



Joel Wuesthoff
Robert Half Legal
Managing Director
Joel.Wuesthoff@RobertHalf.com



Kieran de Terra
Robert Half Legal
Manager, Data Privacy
Kieran.deterra@roberthalflegal.com

Follow updates at WWW.TCBLOG.PROTIVITI.COM



Data Privacy & CCPA

Daniel Campbell, VP Compliance & Audit, CPO, Yardi



YARDI'S ROLE UNDER CCPA

Yardi is a **service provider** under the CCPA.

CCPA provides an exemption for businesses to share
PII with their service providers.

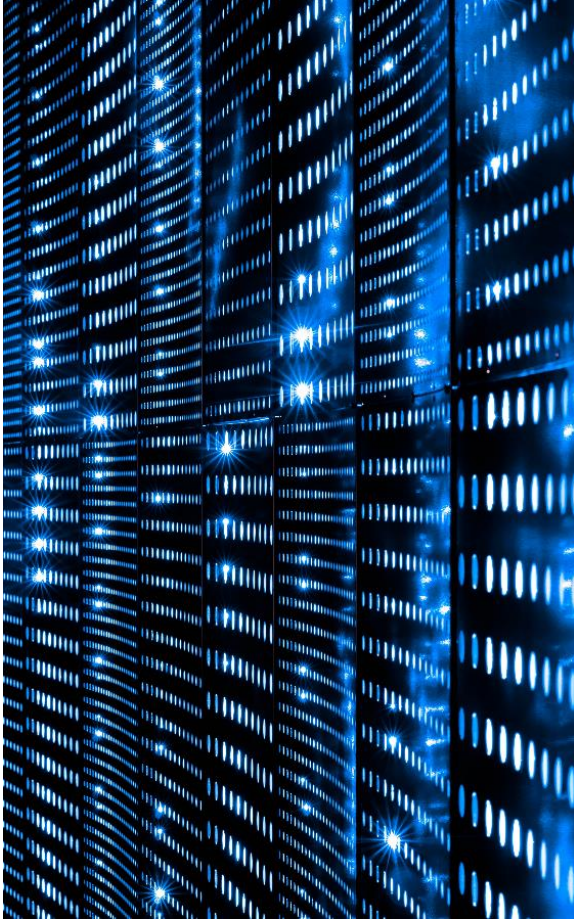




OUR COMMITMENT

- Protecting and **securing** the PII that we process on behalf of our clients
- **Not selling or sharing** any PII that we process on behalf of our clients
- Only using such PII for the specific purpose of **performing services for the client** under the contract and internal operational purposes





EXPERIENCE



GDPR

We implemented policies and procedures for GDPR when it became effective in May 2018.



CCPA

We are well prepared to support our clients' CCPA compliance as well as our own.





Voyager

YARDI VOYAGER TOOLS

FOR CCPA COMPLIANCE



Reporting tool: find all data you hold on an individual



Anonymizer tool: anonymize data on an individual when you receive a request



Similar tools in use in **Europe**



THANK YOU

Please contact us with questions

Daniel Campbell | VP, Compliance & Audit, DPO | daniel.campbell@yardi.com

Jocelyn Belloni | Senior Counsel | jocelyn.belloni@yardi.com

Marketing & Consumer Data Privacy

Christine Walz, Partner, Holland & Knight, LLP



MRI Living Consumer Privacy

MRI Software



Introduction



Marcy Helms

Product Manager, Resident
Engagement

Marcy.Helms@mrsoftware.com



Alycia Workman

Senior Associate General Counsel

Alycia.Workman@mrsoftware.com



Consumer Protection

MRI is committed to enabling our clients to be compliant with various international, national and state/local consumer privacy and protections laws.

Our solution includes:

- Data Consent
- Marketing Consent
- Requesting Anonymization
- Anonymization Process

New features allow for the capture/acknowledgement of consent for personal data being held, opt in/out of marketing and anonymize their personal data on request.

Consumer Protection Laws

MRI monitors various global consumer privacy laws in order to follow the most restrictive policies.

Recent product changes focused on two consumer protection laws:

- GDPR – General Data Protection Regulation implemented by the EU as of May 25, 2018
- CCPA – California Consumer Privacy Act of 2018, effective January 2020

Personal Data

Interaction with personal data occurs at various times in the resident lifecycle, including:

- At the time of application
- Upon application cancelation or denial
- During residency
- Upon move-out
- Upon full disposition of all balances due

Acknowledge Data Consent

- Acknowledging that personal data will be collected
 - Defaults as checked
 - Cannot move forward unchecked, as data should not be saved without consent
- Locations of checkbox for prospects and applicants
 - Phone log
 - Guest card
 - Call Center Agent Dashboard
 - During leasing for added co-residents/other residents in occupants tab

Data Consent Report

- Report all users can run
- Report lists Resident / Applicants / Prospects who have and have not acknowledged data collection
 - Accounts for pre-existing data

Unsubscribe to Communications

- Occupant can elect to opt out of Marketing communication
 - Drop down during leasing in Consumer Privacy tab
 - Drop down in the Resident Lease Information Consumer Privacy tab

Request to be Forgotten

- Request to anonymize information by a Resident / Applicant / Prospect
- Display request to anonymize
 - Date and Time of Request
 - Method of Request
 - Date and Time of Recorded
 - Date completed
- Notification if resident/applicant cannot be anonymized
- Request is recorded and sent to anonymization report and approval workflow
- Anonymization letter can be printed when requested

Approval for Anonymizing Data

- Role based security for final approval
- Committing updates selected residents/applicants/prospects
- Filters at the top of page assist in selection process
- Rule based logic confirms resident/applicant meets anonymization criteria

New Technology, Data Security & Consumer Data Privacy

Moderator: Julianne Goodfellow, Senior Director, Government Affairs, NMHC

Panelists: Josh Erosky, President and Founder, Secure Multi-Family
Kelce Wilson, IAPP and North Texas InfraGard
Scott Lashway, Partner, Manatt, Phelps, & Phillips LLP



CCPA Readiness

Rob Traycoff, Vice President, Associate General Counsel,
RealPage

Aaron Van Patten, Vice President, Product Operations,
RealPage



REALPAGE - CCPA READINESS

California's Consumer Protection Act (CCPA) takes effect January 1, 2020. While not as strict as the European Union's General Data Protection Requirements, CCPA provides the strongest data regulation policy in the United States. California is the first state in the U.S. to pass this form of data protection to protect consumers. Other states are proposing similar regulations to protect consumers as well.

What is CCPA

CCPA applies to companies that conduct business in the state of California or collect or process personal information about California residents. It applies to businesses that meet at least one of the following criteria:

- Generate gross annual revenue of more than \$25 million.
- Buy or share personal information about 50,000 or more consumers, households, or devices.
- Derive at least one-half of its annual revenue from selling consumers' personal information.

Penalties

- Under CCPA, California will impose fines of \$2,500 per incident for unintentional breaches and \$7,500 per incident for intentional violations.
- Consumers can recover up to \$750 per incident, or more if the consumer can show actual damages that exceed \$750. The amounts might seem modest, but CCPA penalties have the potential to be substantial, especially if the CCPA decides on a per-consumer per incident model.



REALPAGE - CCPA READINESS

	CCPA	GDPR
Start date	January 1, 2020	May 25, 2018
Definitions	Protected: "Consumer" Protector: "Business"	Protected: "Data subject" Protector: "Data Controller"
Consumers	California Residents	EU citizens
Companies affected	Any company business in California that: <ul style="list-style-type: none">• Generates more than \$25M annual revenue• Process personal data on 50,000-plus consumers, households, or devices• Derives 50%-plus of annual revenue selling personal data	<ul style="list-style-type: none">• Expanded definition of personal data• Can include photos, medical records, financial status, fingerprints, banking details, and social media posts• Applies to both structured and unstructured data
What it means to consumers	<ul style="list-style-type: none">• Opt out of data collection. (under age 16 must opt in before data collection occurs)• Know what data is collected• Request copy of data• Request deletion of any data collected as of January 1, 2019• Right to non-discrimination	<ul style="list-style-type: none">• Opt in before data collection occurs• Know what data is collected• Request a copy of data• Request deletion of data• Right to restrict processing• Right to object• Right to data portability
Consent	<ul style="list-style-type: none">• Can be established if a consumer signs up or makes an online purchase• Only offers consumer right to opt-out	<ul style="list-style-type: none">• Companies are required to secure consent from consumer via opt-in before collecting data
Response time	<ul style="list-style-type: none">• Response within 45 days for a consumer request	<ul style="list-style-type: none">• Response within 40 days for a consumer request
Penalties	<ul style="list-style-type: none">• Unintentional breach: \$2,500 per incident• Intentional breach: \$7,500 per incident• Damages: \$100 to \$750-plus per incident	<ul style="list-style-type: none">• Fine: Up to the greater of 20 Million Euros or 4% of annual revenue



REALPAGE - CCPA READINESS

Effective January 1, 2020, consumers in California will have broad new privacy rights, and businesses will be subject to new compliance obligations to accommodate those rights.

Does CCPA Apply to RealPage?

- For our direct-to-consumer products, YES.
 - RealPage is subject to all CCPA compliance obligations because RealPage collects personal data directly from California consumers. This means that RealPage will be solely responsible for intake of consumer inquiries and processing of CCPA requests for these products.
- For all other products, RealPage is currently deemed a “service provider” under the CCPA, and as such, RealPage is responsible for supporting our clients’ CCPA compliance obligations. Clients will be required to handle and process consumer CCPA requests directly. RealPage will only be responsible for receiving and processing instructions from our clients.

What is RealPage doing?

RealPage is currently completing a CCPA compliance effort that will support both our direct and indirect compliance obligations commencing on January 1, 2020.

- Personal Data Inventories and Data Mapping
- Product Narratives
- Employee Training
- CCPA Request Processing
- RealPage Service Agreement Updates



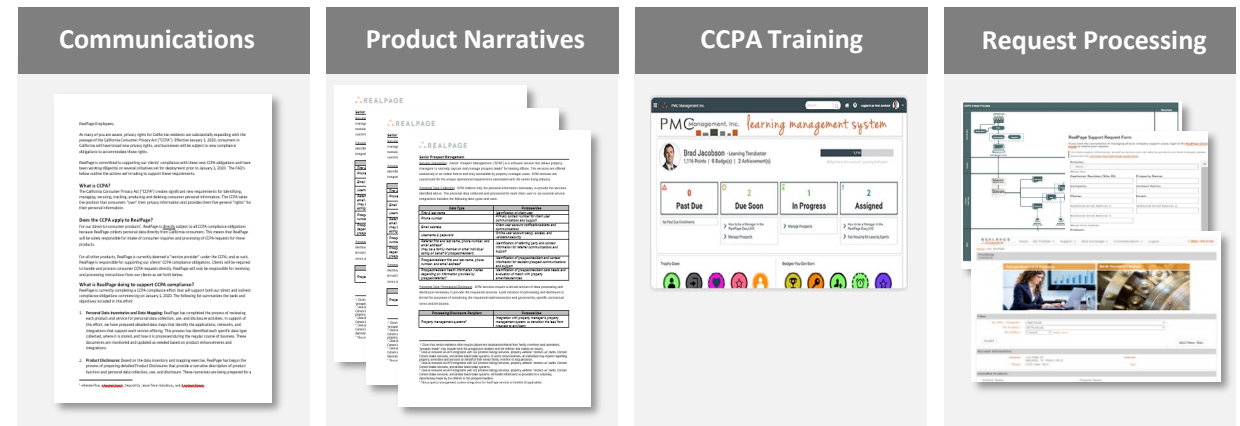
REALPAGE - CCPA READINESS

In April of 2019 RealPage's Product Operations began an assessment of RealPage's products and services to evaluate compliance with the CCPA Requirements and ensure readiness by January 1, 2020. The assessment results defined four work streams: communications, product narratives, training and request processing to ensure RealPage's readiness.

RealPage's CCPA Assessment



Readiness Workstreams



REALPAGE - CCPA READINESS

RealPage is committed to providing the most efficient tools and processes to enable you to meet your CCPA obligations.

- RealPage is an industry leader with decades of experience handling similar requests in the consumer arena with robust controls and processes to ensure that all compliance requests are handled in a timely manner.
- As California finalizes their initial draft of legislative guidance, RealPage is actively monitoring discussions as they unfold to ensure that both RealPage and our partners are fully equipped to be in compliance.
- Our comprehensive solution to the evolving regulatory environment ensures that all CCPA inquiries are properly categorized and expedited through to resolution.



Final Discussion

NMHC White Paper on Data Privacy
nmhc.org/data-privacy

NMHC Staff Contacts:

Kevin Donnelly, Vice President, Government Affairs, NMHC
kdonnelly@nmhc.org

Julianne Goodfellow, Senior Director, Government Affairs, NMHC
jgoodfellow@nmhc.org

Rick Haughey, Vice President, Technology Industry Initiatives, NMHC
rhaughey@nmhc.org

