

ACC NCR FALL CONFERENCE
Advanced Topics for In-House Attorneys

**Employee Privacy: Staying Compliant as
You Transition Out of the Pandemic**

**Baker
McKenzie.**



**Baker
McKenzie.**



Employee Privacy: Staying Compliant as You Transition Out of the Pandemic

ACC NCR Fall Conference
Advanced Topics for In-House Attorneys
September 14, 2022

「Solutions for a
connected world」

Agenda

- 1 Complying with CPRA requirements

- 2 Keeping data secure in remote and hybrid workplaces

- 3 Update on electronic monitoring laws

- 4 Compensation considerations for a distributed workforce

- 5 Staying compliant when collecting DEI data



1

Complying with CPRA requirements

CPRA compliance



Prepare for January 1, 2023 compliance

- CPRA amendments to CCPA take effect **January 1, 2023**; this ends the transitional exemptions for “HR” and “B2B contact information” and includes a 12-month look-back to January 1, 2022.
- Recent efforts to extend HR Data exemptions failed (e.g., AB 1102).
- This means that the scope of information subject to the CPPA will include all employee or human resource-related personal information on January 1, 2023.
- In other words, covered businesses will be required to provide their California employees, contractors, job applicants, and business contacts with the full array of disclosures and rights available to California consumers under the CPRA.
- Businesses must declare on January 1, 2023 in privacy policies whether they have been selling or sharing personal information of employees and B2B contacts in the preceding 12 months and, if yes, offer opt-out mechanisms and alternatives without discrimination.
- Businesses must update service provider agreements, including with recruiters and IT, cloud, payroll, benefits, and other providers.
- Businesses must offer broad access, deletion, rectification, portability and other rights to California employees and B2B contacts, and prepare for what may be the end of confidentiality in the employment area; employers should conduct training, and implement robust data governance policies (including deletion and discovery).

CPRA compliance



Data access / deletion requests from employees

- Under existing employment law, California employees (not contractors) have the right to inspect and receive a copy of the personnel files and records that relate to their performance or any grievance concerning them within 30 days of their written request (this does not extend to records relating to the investigation of a possible crime, letters of reference, or various ratings or reports).
- By contrast, the new “right to know” under the CPRA/CCPA encompasses **two** distinct rights: (i) the right to a disclosure explaining how the employer collects and handles the individual’s personal information; and (ii) the right to copies of “specific pieces of personal information.” The “right to know” applies to California consumers, which goes beyond employees (i.e., including contractors). Employers must generally comply with such requests within 45 days.
- The “right to know” is not absolute, and employers can refuse if the request is manifestly unfounded or excessive (e.g., if the purpose is to harass) and does not cover privileged information (e.g., communications with in-house and external counsel).
- The CPRA/CCPA introduce a new right to “data deletion” (also not an absolute right). An exception should apply for most categories of personal information reasonably necessary to managing or administering current or past employment or contract work relationship.
- The CPRA/CCPA gives California residents other rights including the right to limit the processing of sensitive information. There are exceptions to the right to limit the processing of sensitive information, but none of the statutory exceptions apply squarely to HR data.

HR Data

Proposed steps to complete before January 1, 2023



Notice

Conduct factual due diligence for HR data re: data collection, use, disclosure, and retention.

Update the HR privacy notices with additional information on CCPA/CPRA rights, including updates to the Employee Privacy Notice that disclose the processing of sensitive personal information.

Include notice on collection, use, disclosure, and retention



Access and Correction

Prepare for and provide employees and other covered individuals with access to and right to correct their personal information upon verifiable request.

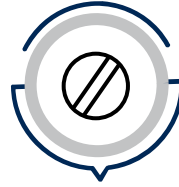
Develop a system to streamline process for assisting with access requests.



Deletion

Prepare for and provide employees/contractors with the opportunity to delete their personal information, subject to exceptions to perform a transaction, comply with regulations, detect and protect against data security incidents, and the like.

Develop a system to streamline process for assisting with deletion requests.



Opt-outs/Limits

Prepare for situations (if any) where disclosure of HR Data to other businesses or third parties would constitute a "sharing" or a "sale."

Provide ability to limit use and sharing of sensitive personal information.

Review and update agreements with service providers, contractors, and third parties.



Non-Discrimination

Confirm that there is no discrimination against any employee or other individual due to the exercise of their rights under CPRA.

B2B Data

Proposed steps to complete before January 1, 2023



Notice/Terms

Conduct factual due diligence for B2B data re: data collection, use, disclosure, and retention.

Update the B2B privacy notices with additional information on CPRA rights.

Update contracts with clients in the B2B space (e.g., 401k, financial advisory, and the like).



Access and Correction

Prepare for and provide B2B contacts with access to their personal information and right to correct any inaccuracies upon verifiable request.

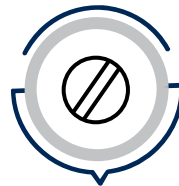
Develop a system to streamline process for assisting with access and correction requests.



Deletion

Prepare for and provide B2B contacts with the opportunity to delete their personal information, subject to exceptions to perform the transaction, comply with regulations, detect and protect against data security incidents, and related exceptions.

Develop a system to streamline process for assisting with deletion requests.



Opt-outs/Limits

Prepare for situations (if any) where disclosure of B2B Data to other businesses or third parties would constitute "sharing" or a "sale".

Provide B2B contacts ability to limit the use and disclosure of sensitive personal information.

Review and update agreements with service providers, contractors, and third parties.



Non-Discrimination

Confirm that there is no discrimination against any B2B contact due to the exercise of their rights under CPRA.

Proposed steps to complete before January 1, 2023



Notice

Assist with updating privacy notices on web and mobile app properties with additional information on CPRA rights and other content.



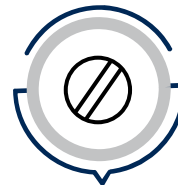
Access and Correction

Assess readiness of tools and systems to address rights to access and/or correct personal information.
Confirm and/or enhance tools and systems as needed.



Deletion

Assess readiness of tools and systems to provide opportunity to request deletion of personal information, subject to exceptions to perform the transaction, comply with regulations, detect and protect against data security incidents, and related exceptions.
Confirm and/or enhance tools and systems as needed.



Opt-outs/Limits

Assess readiness of tools and systems to provide opportunity to allow users to opt-out of the "sale" or "sharing" of personal information, as well as to limit use and disclosure of any sensitive personal information.
Confirm and/or enhance tools and systems as needed.

Other Privacy Law Updates



Beyond California, four (4) other states have already adopted comprehensive data privacy laws focused on consumers (excluding HR and B2B)

- Virginia Consumer Data Protection Act (effective January 1, 2023)
- Colorado Privacy Act (effective July 1, 2023)
- Connecticut Data Privacy Act (effective July 1, 2023)
- Utah Consumer Privacy Act (effective December 31, 2023)



25+ other states considering comprehensive data privacy laws





The Federal Trade Commission has initiated rulemaking on “commercial surveillance and data security”



Federal legislation is under active consideration, including the bipartisan bill entitled the American Data Privacy and Protection Act



Other US State Privacy Laws: Key Differences

	 Important Dates	 Key Differences Compared to CCPA/CPRA
Virginia Consumer Data Protection Act	Effective Date: January 1, 2023	<ul style="list-style-type: none"> ▪ Carves out persons acting in a commercial or employment context (i.e., B2B and HR contacts). ▪ Does not have any provisions that address opt-out preference signals. ▪ Requires that controllers obtain opt-in consumer consent to process “sensitive data”. ▪ 30-day cure period before AG can initiate an enforcement action. ▪ No private right of action.
Colorado Privacy Act	Effective Date: July 1, 2023	<ul style="list-style-type: none"> ▪ Carves out persons acting in a commercial or employment context (i.e., B2B and HR contacts). ▪ Requires that controllers obtain opt-in consumer consent to process “sensitive data”. ▪ 60-day cure period prior to initiating an enforcement action “if a cure is deemed possible”. ▪ No private right of action.
Utah Consumer Privacy Act	Effective Date: December 31, 2023	<ul style="list-style-type: none"> ▪ Carves out persons acting in a commercial or employment context (i.e., B2B and HR contacts). ▪ No right to correction. ▪ Narrower right to deletion - consumers in Utah only have the right to delete personal information that the consumer provided to the controller. ▪ Does not require controllers to provide a process for consumers to appeal denials of requests. ▪ Does not require that businesses conduct data protection assessments. ▪ No private right of action.
Connecticut - S.B. 6, An Act Concerning Personal Data Privacy and Online Monitoring	Effective Date: July 1, 2023	<ul style="list-style-type: none"> ▪ Carves out persons acting in a commercial or employment context (i.e., B2B and HR contacts). ▪ Requires that controllers obtain opt-in consumer consent to process “sensitive data”. ▪ 60-day cure period prior to initiating an enforcement action. ▪ No private right of action.



2

Keeping data secure in remote and hybrid workplaces

Hybrid workforce privacy considerations

Things to keep top-of-mind

Consider:

Concerns for employees working from home and employees returning to the workplace both apply

Because hybrid employees are frequently in both places (home and the worksite), both sets of considerations apply.

Working from a personal device

Confidential information could be obtained by hackers or lost because of lack of appropriate backup.

Accessing company data on multiple devices/from multiple locations

Employees logging on from home and from work can open up the company to more cybersecurity risks. Employees should be required to follow company IT policy and use secure connections (VPN, etc.).

Use of flash drives

Employees may be tempted to use flash drives to store information for ease of use between home and the workplace, but flash drives can be lost and are vulnerable to hacking.

Working from the local drive

Employees may be tempted to save files on a local drive on a machine they're carrying back and forth to work (especially if it takes awhile to log onto the company's secure network), making sensitive company information vulnerable.

Carrying trade secret/confidential hard copies

Employees working between home and the worksite may be tempted to carry hard copy files back and forth, risking lost or misplaced confidential documents.

Know the privacy laws that apply

Understand and address privacy regulatory issues



Notice and consent requirements

- Privacy laws may require that employees be notified that their personal data is transferred to third countries
- Certain jurisdictions may require employee consent to transfer their data to third countries
- Certain categories of personal data may be subject to additional transfer restrictions



Data Transfer Restrictions

- European Union and other jurisdictions are placing increasing requirements on organizations transferring personal data to third countries
- Schrems II transfer impact assessments



Data localization requirements

- EU policymakers considering elements of data localization that would result in stricter limitations to trans-Atlantic data flows
- Some countries have data localization requirements (e.g. Vietnam, Indonesia, China, Brazil, India, Australia, Korea, Nigeria and Russia)



Employee privacy considerations checklist

What to think about when collecting/processing employee data

- ✓ **Informed consent:** Have employees been notified of the existence and purpose of the data collection and processing? If necessary, have employees given consent, and has this consent been documented?
- ✓ **Proportionality:** Is the data collection proportional to the purpose for which it's being used? Data aggregation, anonymization, and minimization may mitigate an employer's exposure to data privacy liability—consider whether these principles can be applied while preserving the adequacy of the data for the specific purpose.
- ✓ **Legal basis:** Some jurisdictions require that an employer have a legal basis to collect personal information. If such restrictions apply, ensure that such a basis exists.
- ✓ **Data transfers:** If employee data is to be transferred between sites, are specific data transfer mechanisms required (especially in light of Schrems II)? Are appropriate terms in place with vendors and other third parties handling the data? Do data localization regimes restrict the transfer of data outside the jurisdiction?
- ✓ **Data security:** Ensure that any data collected is stored securely and ensure that access is strictly limited to those who require the information. Adopt particular security measures for sensitive data such as health or diversity data and understand whether specific security measures are mandated by law for such special categories.

Implement formal policies and procedures



Disclose and document

- Disclose to employees how you collect, process and share their personal data
- Use formal consent policies that are compliant with relevant laws
- Review and update policies on a regular basis
- Provide training to employees so they understand their data protection rights



3

Update on electronic monitoring laws

What is electronic monitoring?



Keeping on top of what your employees are doing

- Electronic methods employers use to surveil their employees' whereabouts and activities
- Includes
 - Tracking employee locations through IP addresses or GPS location tracking
 - Tracking when employees come and go with time clocks, employee badges, etc. or collecting biometric information
 - Systems that track workers' activity via desktop monitoring, including keystroke tracking, mouse tracking, video surveillance and other digital tools

New York State's Electronic Monitoring Law



Amendments to Civil Rights Chapter 6, Article 5, Section 52-C*2

- Requires private employers in New York (regardless of size) to (1) provide employees with a notice of electronic monitoring, (2) obtain proof of acknowledgement, and (3) prominently post the notice for all to see
- Requires compliance if employers monitor / intercept telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage of or by an employee of any electronic device or system (including the use of a computer, telephone, wire, radio, or electromagnetic, photoelectronic, or photo-optical systems)
- Covered employers must give written notice upon hiring to all employees subject to electronic monitoring, and obtain acknowledgement from employees (in writing or electronically)
- Exceptions: Employers are not required to comply with the law's disclosure obligations if the monitoring activities are designed to manage the type or volume of incoming or outgoing email, voicemail or internet usage; are not targeted to monitor or intercept data / usage of a particular individual; and are performed solely for the purpose of computer system maintenance and/or protection
- Employers who violate the law may be fined \$500 for a first offense, \$1,000 for a second, and \$3,000 for all subsequent offenses

Electronic monitoring of employees

Legal Issues:

Make sure to comply with your jurisdiction's rules

Monitoring what's on an employee's computer screen, internet activity, e-mails, etc. on devices owned by the employer during work hours is fine in many states BUT check your jurisdiction.

Provide notices to employees

Employees should be provided with clear notices that they're being monitored. Monitoring of employees in general is subject to high requirements due to intrusiveness and impact on employee's privacy

Obtain consent

If it's an employee-owned device, make sure you have proper consent from the employee to allow the use of their device for monitoring. Be aware of restrictions on validity of employee consent outside of the US.

Operational Issues:

Be proportionate

Keep it limited to the purpose (such as to maintain the integrity of hardware/software from malicious cyber activity or to protect trade secrets). Don't step over the line into an invasion of privacy.

Protect data obtained

Protect any information you've obtained regarding employee behavior and use it only for the purpose for which it was obtained.

Use passwords for monitoring

Make your databases containing company information password-protected, with each employee using a unique password that he or she is prohibited from sharing with others. This will enable you to monitor your employees' access to company information and flag suspicious activity like mass downloading or sharing.



4

Compensation considerations for your distributed workforce

Pay transparency laws



What we're seeing now and what's trending

- Increase in state / local laws requiring that employers disclose the compensation rate or range for a position in the job posting (including California, Colorado, Washington, and New York City). Examples:
 - Colorado's Equal Pay for Equal Work law requires employers to list the hourly rate or salary (or range) for the position and a general description of the benefits and other compensation offered for the position for both internal and external job postings
 - Effective November 1, 2022 it will be an "unlawful discriminatory practice" under the New York City Human Rights Law for an employer to advertise a job, promotion, or transfer opportunity without stating the position's minimum and maximum salary in the job advertisement
 - On August 30, 2022, the California legislature passed SB 1162, which would require California employers with 15 or more employees to include the salary or hourly wage range of positions in job listings. Governor Newsom has until September 30, 2022 to sign the bill into law.

Pay adjustments for geography



Best practices and considerations

- Consider putting a geographic pay policy in place, especially if full-time remote work is continuing to rise
- Choose a metric for determining pay differences and how you will apply the pay differentials and apply it across-the-board
 - Cost of labor v. cost of living
 - Pay differentials as a premium/discount to a jobs-based pay structure or to individual pay, or separate base pay structures for each different geographic location where employees are working
- Consider how lowering pay—even for a lower cost geographical area—will affect retention
 - Is the job market national (like tech), with market rates trending toward a national market demand?

According to WorldatWork's Geographic Pay Policies Study (February 2021), 67 percent of employees expected their compensation to reflect their location.

<https://worldatwork.org/workspan/articles/remote-work-raises-geographic-pay-policy-questions>



Jurisdictional requirements



Know applicable law where your employees are located

- There are increased security and confidentiality risks when paying a distributed workforce, as well as regulations that change from country to country
- Consider:
 - Corporate presence requirements (to establish payroll)
 - Regulations surrounding payroll
 - Tax considerations
 - Data security concerns (increased risk of exposure of employee confidential wage / salary information)



5

Staying compliant when collecting DEI data from employees

Collecting and documenting diversity data

Mitigate risks and pitfalls in privacy



Determine what diversity information the company needs and whether it can be lawfully and successfully collected.

- Don't collect more than you need
- Be aware of issues associated with collecting certain data information outside of the US
- Gender data can generally be collected in and outside of the US
- Consider the robustness of the data before analyzing it and drawing conclusions (i.e., what percentage of the population has self-identified)
- Data collection can be fraught with potential risk, cost and complexity. This is magnified when a company has global operations with jurisdictions having different rules and regulations
- Be aware of how data looks not only internally, but also externally if disclosed / obtained through FOIA
 - Federal contractors submitting EEO-1 data have until September 19 to object to the OFCCP's public disclosure of EEO-1 data

Collecting and documenting diversity data

Where are you collecting data?

■ California

- CCPA requires notices “at collection.” CCPA “opt out” rules (as of Jan. 1, 2023): CA residents will have the right to request that businesses stop using their “sensitive personal information,” including information about racial or ethnic origin, for purposes outside of various narrow exceptions.

■ Europe

- Under Article 9(1) of the GDPR (including as currently operative in the UK) processing special categories of personal data — including information about racial or ethnic origin and data concerning a natural person’s sex life or sexual orientation — is prohibited unless an exception applies (such as consent or where processing is necessary to carry out legal obligations, including in the field of employment).

■ Asia-Pacific

- Employers are generally legally permitted to collect D&I data, including ethnicity data, about their workforce for D&I program purposes. In a few jurisdictions, it is required that employers collect and sometimes publicize such data.

■ Latin America

- Subject to notice and, in some cases, consent, employers in Latin America are generally permitted to collect personal data for D&I program purposes—and in some cases are legally required to collect it.

Collecting and documenting diversity data

Mitigate risks and pitfalls in privacy



Develop a cohesive strategy around privilege and confidentiality.

- Collected employee information regarding race/gender or other protected categories should be stored outside of employee's personnel file
- Analyses of diversity data should be conducted under attorney client privilege:
 - Analyses should be at the direction of internal/external counsel;
 - Project team members should be limited to only those who are essential;
 - A privilege memo should be issued to team members at the start of the project describing the privileged nature of the project and the steps each team member must take to protect the privilege;
 - Final analyses should not be widely disseminated.
- Analyses that will be publicly released (e.g. ESG analyses) should be conducted separately from privileged analyses.
- Beware of possible threats to attorney-client privilege (such as the OFCCP's March 2022 directive notifying of increased scrutiny of federal contractors' pay equity audits, and taking the position that contractors' pay equity analyses are not privileged)



6

Appendix



A

Complying with the CCPA and CPRA

CCPA / CPRA compliance



Record retention / deletion

- Current record **retention** requirements:
 - Employers must retain personnel records for applicants and employees for 4 years from the date the records were created or received, or the date the employment action was taken (previously 2 years).
 - Employers must maintain a copy of each employee's personnel records for at least 3 years after termination of employment.
 - Employers must maintain payroll records, job classification, and other terms and conditions of employment for a period of no less than 3 years after the creation.
 - Record retention requirements can be longer in some instances (e.g., work-related injuries and illness, records of employee exposure to hazards, litigation, etc.).
- Current record **deletion** requirements:
 - California employment law does not specify any requirements regarding the destruction of records.
 - Privacy laws, however, require that personal information not be kept longer than necessary or as required by law.
 - CPRA provides that "a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal. information was collected for longer than is reasonably necessary for that disclosed purpose."



B

Keeping data secure in remote and hybrid workplaces

Remote workforce privacy considerations

Permanent remote workers

Consider:

Handling of trade secrets

How they should be labeled, where they should be maintained, which employee groups will have access to them, what procedures will be implemented to ensure their security.

Confidentiality/Non-Disclosure

If employees will have access to trade secrets/confidential information, be sure to include confidentiality and non-disclosure provisions.

Remote access and authorization

Make sure you develop protocols in the policy for remote access to company databases. Ensure that only authorized users have access to your network.

Handling of sensitive hard copy documents

Prohibit the printing or copying of significant company materials without express authorization, or requiring telework employees to keep all hard-copy materials in a locked cabinet when not using them.

Outline the company's responsibilities

Any technical support provided to the employee; work expenses the employer reimburses; and equipment the employer provides and repairs (computers, cell phones, teleconferencing equipment, facsimile equipment, anti-virus software, office supplies).

Distribution and signature

Require teleworking employees to sign (even e-sign) the policy before granting remote access to confidential information. This may be an opportunity to include requisite Defend Trade Secrets Act language.

Cybersecurity Considerations

From network security to home security

- Remind employees that sharing company information through non-company applications such as personal email accounts, text messaging, etc. is prohibited.
- Appropriate encryption should be used.
- Transmit substantial amounts of company information only through secured company servers.
- Employees should have a secure workspace with reliable connectivity (not local café).
- Employees should be required to connect to VPN first.
- Conversations should be secured from eavesdropping (not in the range of virtual assistants or other IoT listening devices such as Alexa, GoogleHome, etc.).
- Keep work devices secure. Require the employee to agree that no family members or others will access company issued work devices or personal devices used for work.
- Keep physical workspaces secure. Require employees to include elements of traditional security to the home office (locked cabinets, locked desk drawers, passwords, remove IoT devices).
- Consider providing/reimbursing for equipment needed to ensure security (filing cabinets, separate printers, shredder).



Update on electronic monitoring laws

Electronic monitoring laws



Other states

- **Connecticut** employers engaging in electronic workplace monitoring are required to provide written notice to employees and post the notice in a conspicuous place (see Conn. Gen. Stat. Ann. § 31-48d(b)(1))
- **Delaware** employers generally cannot monitor employees' telephone or computer use without providing advance notice of the monitoring-either daily through electronic notice each time the employee accesses the employer-provided email or internet, or through a one-time notice (in writing, in an electronic record or another electronic form) and acknowledged by the employee in writing or electronically (see 19 Del C. § 705(b))
- **California** employers are prohibited from eavesdropping on or recording employees' private telephone, email, or in-person conversations without prior consent by all participants (see Cal. Penal Code §§ 631(a) and 632(a))
- In **Texas**, employers are prohibited from intercepting or disclosing the contents of wire, oral, or electronic communications without prior employee consent (see Tex. Penal Code Ann. § 16.02). An employer may monitor its own phone system under the "business extension exception" to the federal wiretapping law (18 U.S.C. § 2510(5)(a)), but must inform employees that this monitoring may be taking place
- Many states have not specifically addressed employer monitoring, but have other strict privacy laws that may consider an employer monitoring their employees' communications to be an invasion of privacy



D

Staying compliant when collecting DEI data from employees

Collecting and documenting diversity data



Create a DEI data protocol with a sound data-retention policy

- Identify the members of your project team, including a well-trained “data protocol officer” who is in charge of properly gathering and using sensitive information
- Clarify who is authorized to analyze the data
- Establish a procedure for adding new members to the team
- Delineate the scope of the team’s work
- Clarify that nobody may share sensitive information outside the team without the data protocol officer’s approval
- Clarify that violation of the protocol may lead to disciplinary action
- Anyone with access to diversity metrics must be trained to know what is and isn’t permitted
- Most companies already have a policy in place regarding how long to keep other kinds of data. If possible, adapt the policy you have in place regarding how long to keep other kinds of data for use with DEI data
- Make sure that your policy complies with local and other laws
- Follow the general principle that you should retain your data only as long as necessary to identify problems and measure the effectiveness of specific DEI interventions



E

Compensation considerations for your distributed workforce

Pay transparency laws



Handling new pay transparency obligations

- Key takeaways / tips:
 - Assemble a cross-functional team to review the company's process for determining compensation to ensure reliance on relevant job-related factors
 - Set or review compensation rates or ranges for all positions and ensure that job descriptions and other documents are consistent with them
 - Develop a comprehensive pay disclosure policy that addresses varying state and local requirements
 - Develop consistent standards for publishing internal and external job postings
 - If using pay ranges, ensure a consistent approach to determining the amount offered to any candidate
 - Communicate the new policy to existing employees
 - Train managers on policy requirements
 - Partner with counsel for an internal audit to identify pay inequities

Questions



Speakers



Krissy Katzenstein
Baker McKenzie
Partner, DC/NY
T +1 212 626 4364
krissy.katzenstein@
bakermckenzie.com



Karen Moore
Unisys Corporation
Chief Compliance Officer
and Privacy Counsel
T +1 301 655 5187
karen.moore@
unisys.com



Veronica Torres
Jumio
Worldwide Privacy and
Regulatory Counsel
T +1 202 441 1971
veronica.torres@
jumio.com



Harry Valetk
Baker McKenzie
Partner, NY
T +1 212 626 4285
harry.valetk@
bakermckenzie.com



Krissy Katzenstein

Baker McKenzie
Partner, DC/NY
T +1 212 626 4364
krissy.katzenstein@
bakermckenzie.com

Krissy Katzenstein is a partner in the Employment & Compensation Practice Group in Baker McKenzie's New York office. Krissy represents employers in a wide range of employment disputes, with a focus on class and collective actions involving systemic discrimination as well as federal and state agency investigations of systemic discrimination and harassment claims. Krissy was named a "Rising Star" in Employment Law by Law360 in 2019.



Karen Moore

Unisys Corporation
Chief Compliance Officer
and Privacy Counsel
T +1 301 655 5187
karen.moore@
unisys.com

Karen Moore is the Chief Compliance Officer and Privacy Counsel at Unisys Corporation, a global technology service and solutions company (NYSE: UIS). Reporting to the General Counsel and to the Board Audit & Finance and Security & Risk Committees, she is responsible for the design and implementation of the company's global compliance program and charged with oversight of the Unisys cross-functional privacy program. Currently based in the Washington DC metro area, Mrs. Moore has also lived and worked in Moscow, Russia, and Lausanne, Switzerland.

**Veronica Torres****Jumio**Worldwide Privacy and Regulatory
Counsel

T +1 202 441 1971

veronica.torres@
jumio.com

Veronica Torres is the Worldwide Privacy and Regulatory Counsel and Data Protection Officer for Jumio, leading Jumio's global privacy program and data protection strategy. Her prior experience includes working with start-ups, federal agencies, and Fortune 500 companies in developing privacy programs, advising on third-party risk, and navigating emerging technologies in an evolving privacy landscape. She serves on the IAPP's Privacy Bar Advisory Board. Veronica earned her J.D. from Brooklyn Law School and B.A. in Political Science from American University. She is CIPP/US certified and has been around privacy so long to see her CIPP/G discontinued. If you're in DC, you can find Veronica exploring local bike paths and restaurants.

**Harry Valetk****Baker McKenzie**

Partner, NY

T +1 212 626 4285

harry.valetk@
bakermckenzie.com

Harry A. Valetk is a partner in the Global Privacy and Security Practice group based in New York, advising global organizations on privacy and data security compliance requirements. He regularly supports companies in financial services, retail, pharmaceutical/ healthcare, travel/hospitality, cloud technology, and manufacturing industries. His practice is focused on delivering commercially practical advice to highly regulated companies on designing security, privacy, and technologically compliant solutions. Harry's practice routinely covers a wide range of issues on global regulatory implementation readiness for privacy laws, including GDPR, CCPA, CPRA, HIPAA, GLBA, the Children's Online Privacy Protection Act (COPPA). He also works with companies in developing customized comprehensive incident response plans, trainings, table-top exercises, and advising senior management on liability risk mitigation.



Baker McKenzie offers clients integrated solutions to complex legal challenges.

Our unique culture, developed over 70 years, enables our 13,000 people to work together across borders and practice areas. We provide seamless advice underpinned by local market knowledge and deep sector expertise so that business leaders can feel confident in driving growth that is both sustainable and inclusive.

bakermckenzie.com

© 2022 Baker McKenzie. All rights reserved. Baker & McKenzie International is a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner or equivalent in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.