APRIL 2023

CLEARSTAR®

SCREENING COMPLIANCE UPDATE

CLEARSTAR OFFERS EEOC GUIDELINES COMPLIANCE ON CRIMINAL BACKGROUND CHECKS, GDPR & SOC TYPE 2 SECURITY CONTROL COMPLIANCE AND STAFFING COMPLIANCE.

Compliance is one of the most important parts of background screening, it involves following the rules and regulations set forth by the Fair Credit Reporting Act and local ordinances.

CLICK FOR PAST UPDATES

CLEARSTAR®

TABLE OF CONTENTS

SCREENING COMPLIANCE UPDATE | APRIL 2023

ClearStar is happy to share the below industry related articles written by subject matter experts and published on the internet in order to assist you in establishing and keeping a compliant background screening program.

FEDERAL DEVELOPMENTS

Employers Must Update Their Summary of Rights Notice for Background Check Screenings

Employers should promptly update their Summary of Consumer Rights notice provided to applicants and workers before taking adverse employment action based on their background check reports, thanks to a new rule about to take effect. On March 17, the Consumer Financial Protection Bureau (CFPB) released an updated "Summary of Your Rights Under the Fair Credit Reporting Act" notice for consumer reporting agencies and background check users to incorporate into their screening processes. While the CFPB's final rule is set to take effect on April 19, the agency has provided a grace period for mandatory compliance until March 20, 2024. What should employers do in order to get into compliance?

Quick Background on the Summary of Consumer Rights Notice
Most employers are aware that they need to comply with certain legal requirements when obtaining background checks and when taking an adverse employment action (such as rejecting an applicant, revoking a conditional offer of employment, or terminating a worker), in response to negative information obtained on a background check. Before employers can take an adverse employment action, based in whole or in part, on information in a background check report, the Federal Fair Credit Reporting Act (FCRA) requires employers to follow a pre-adverse/adverse action process. During this process, employers are required to provide applicants and workers with: (1) a copy of their report, (2) a summary of their rights under the FCRA, and (3) other FCRA information.

The CFPB, the federal agency that oversees procedures used in background screening processes, maintains a standardized summary of consumer rights notice titled, "A Summary of Your Rights Under the Fair Credit Reporting Act," which employers must use to comply with their requirements.

Revised Template: What Changed?
The updates to the CFPB's March 17 Summary of Rights Notice that employers (and consumer reporting agencies) should begin using to satisfy FCRA requirements are largely non-substantive in nature. For example, they include formatting corrections and updated contact information for the CFPB and other federal agencies. The CFPB also revised the document to remove obsolete business types such as "Federal Land Banks."

Those who began using the updated notice immediately should be aware that when it was published on March 17, the notice omitted a phone number for applicants and workers to use when seeking to limit "prescreened" offers of credit and insurance based on their report. The original notice listed 1-800-XXX-XXXX as the phone number to use. However, the CFPB has since corrected the notice, inserting the appropriate contact information: 1-888-567-8688. You should check to make sure you are using the corrected notice.

When Should You Start Using It?
While the CFPB's final rule becomes effective April 19, the mandatory compliance date is a year away (March 20, 2024). Regardless, we recommend that you begin using the updated notice as soon as possible to get ahead of the compliance deadline and ensure that applicants and workers are provided the correct contact information for the agencies listed in the notice.

Notably, you do not need to provide the updated notice to anyone who you have already given the prior notice. You should simply ensure that you are using the most current version of the notice moving forward.
CLICK HERE.

Treasury Greenbook Includes Proposal to Alter Work Opportunity Tax Credit

On March 9, 2023, the U.S. Department of Treasury released the Greenbook (formally known as the General Explanation of the Administration's Revenue Proposals) for FY 2024 to explain revenue proposals included in the Administration's budget. One proposal is to increase the number of hours required to be worked by an individual for the employer to be eligible for the Work Opportunity Tax Credit (WOTC).

The WOTC generally provides a tax credit equal to 40 percent of qualified wages paid in the first year of employment for employers who hire individuals from one or more of 10 targeted groups. Currently, the WOTC credit is reduced to 25 percent of qualified wages if the individual works between 120 and 400 hours in the first year of service. The WOTC does not apply if the individual works fewer than 120 hours in the first year of service.

The WOTC applies to individuals from the following groups: (a) recipients of Temporary Assistance for Needy Families; (b) veterans; (c) people recently convicted of, or released from incarceration for, a felony; (d) residents of an empowerment zone or a rural renewal community who are at least 18 but not yet 40 years old; (e) referrals from State-sponsored vocational rehabilitation programs for the mentally and physically disabled; (f) summer youth employees who are 16 or 17 years old residing in an empowerment zone; (g) Supplemental Nutrition Assistance Program benefits recipients at least 18 years old but not yet 40 years old; (h) Supplemental Security Income recipients; (i) long-term family assistance recipients, and (j) long-term unemployment recipients. An individual must be certified by a designated local agency as a member of a targeted group. For most groups, qualified first-year wages are capped at $6,000; however, the cap is as high as $24,000 for long-term unemployed veterans who are disabled.

The Administration's proposal would raise the minimum number of hours worked in the first year of service by an individual to 400 hours for an employer to be eligible for the WOTC. This would eliminate the 25 percent tax credit provided under current law if the individual worked between 120 and 400 hours. The proposal would be effective for individuals hired after December 31, 2023, and seeks to align the credit with the WOTC's goal of providing long-term employment opportunities for members of targeted groups. By establishing a 400-hour threshold to qualify for the WOTC and eliminating the incentive for fewer hours worked, the Administration hopes to encourage employers to hire more permanent rather than temporary employees.
CLICK HERE.

The EEOC Continues to Push Enforcement of Anti-Discrimination Laws In Relation to Employers' Use of Artificial Intelligence ("AI") In Hiring

On March 23, 2023, the EEOC announced a conciliation agreement with DHI Group, Inc. ("DHI")—a company that operates a job-search website (Dice.com) for technology professionals. The conciliation arose out of multiple national discrimination charges that had been filed against DHI Group, Inc. because its customers posted positions on the website that excluded Americans—thereby deterring individuals from applying based on their national origin.

Pursuant to the conciliation agreement, DHI agreed to:

- Rewrite its programming to scrape for potentially discriminatory keywords such as "OPT"[1], "H1B"[2] or "Visa" that appear near the words "only" or "must" in its customers' new job postings.
- Revise its guidance to customers on its "Job Postings not permitted on Dice" website pop-up to include instructions to avoid language such as "H-1Bs Only" or "H-1Bs" and OPT Preferred."

This conciliation agreement follows the EEOC's May 12, 2022 guidance concerning potential discrimination against disabled employees via the use of AI,[3] its January 10, 2023 draft Strategic Enforcement Plan which emphasizes its focus on eliminating barriers to recruitment and hiring resulting from AI,[4] and its January 31, 2023 hearing concerning employment discrimination and the use of AI.[5]

Given the EEOC's increased focus in this area, employers must be cognizant of the potential for costly class-based litigation concerning the use of AI technology.

Employer Tips to Reduce Risk Related to the Use of Artificial Intelligence in Hiring

- *If using an outside resource to assist with hiring, ask them whether the software they employ and algorithms that are used have been tested for potential bias and what steps have been taken to eliminate the same.*
- *Thoroughly review potential job postings to evaluate whether the language used may have the potential to screen out applicants based on protected characteristics. In this case, what may have seemed to be innocuous at the time (language that ensured the applicant was legally able to perform work in the United States) ended up screening out an entire protected class.*

CLICK HERE.

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

Iowa is the Sixth U.S. State that Enacts Data Privacy Law

Iowa is now the sixth state in the U.S. to adopt a comprehensive privacy law that aims to give consumers more control over protecting their personal data.

Signed by Gov. Kim Reynolds (R) on Tuesday, Senate File 262 was unanimously passed by the Iowa Senate and House. The law will go into effect on January 1, 2025. The law joins data protections in California, Colorado, Connecticut, Utah, and Virginia adopted.

Iowa's data privacy law applies to companies that (1) control or process data of at least 100,000 Iowa consumers, or (2) control or process data of at least 25,000 Iowa consumers and derive 50% of their revenue from the sale of personal data.

Notably, Iowa joins the other five states (i.e. California, Colorado, Connecticut, Utah, and Virginia) by exempting data regulated by the Fair Credit Reporting Act (FCRA). There are also exemptions for state and municipal entities, political subdivisions, banks, and financial companies subject to the Gramm-Leach-Bliley Act (GLBA), and healthcare organizations as specified in the statute subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), non-profits, higher education institutions including Family Educational Rights and Privacy Act (FERPA) data, data governed by the Children's Online Privacy Protection Act of 1998 (COPPA) and certain information related to employment.

Under the Iowa law, consumers are provided with four main rights: the right to access, the right to delete, the right to portability and the right to opt out of the sale of their personal data. Like the state privacy laws enacted by Colorado, Connecticut, Virginia and Utah, the Iowa privacy law does not offer a private right of action. It does, however, provide the attorney general with the exclusive right to enforce the act through civil investigative demands. The attorney general must provide the violating party with a written notice listing the violations and, with 90 days to cure the violations, notify the attorney general of the cure and provide a statement that no further violations will occur. The Attorney General may seek monetary damages of up to $7,500 per violation of the law and injunctive relief.
CLICK HERE.

Data Breach Notification Law Update: Utah and Pennsylvania

For businesses subject to data breach notification requirements in Utah and Pennsylvania, a series of significant amendments will soon go into effect in both states. Below is a summary of those amendments.
Amendments to Utah Data Breach Response Law

The Governor of Utah signed S.B. 127 into law on March 23, 2023, amending state data breach disclosure requirements and creating a new state "cyber center" tasked with receiving and managing breach disclosures,[1] collaborating with state and federal agencies in the development of cybersecurity incident response measures,[2] and developing a statewide strategic cybersecurity plan by June 2024,[3] along with other duties. The amendments take effect in early May.

Noteworthy aspects of the amendments include:

- Required reporting of a "system security breach" to both the Office of the Attorney General and the newly created Utah Cyber Center when an investigation of the breach "reveals that the misuse of personal information relating to 500 or more Utah residents, for identity theft or fraud purposes, has occurred or is reasonably likely to occur."[4] Where 1,000 or more Utah residents are affected by such a breach, covered entities also must notify consumer-reporting agencies. [5] These new notification requirements will go into effect in early May 2023. Presently, Utah's data breach notification statute has no requirement to notify government agencies or consumer reporting agencies.
- The creation of the Utah Cyber Center, which is responsible for, among other things, developing "incident response plans to coordinate federal, state, local, and private sector activities and manage the risks associated with an attack or malfunction of critical information technology systems within the

state."[6]

- A requirement that governmental entities notify the Utah Cyber Center "as soon as practicable" when the entity becomes aware of a system security breach.[7] Once notified, the Cyber Center will be tasked with providing assistance to the government entity in responding to the breach, which may include conducting "all or part" of the breach investigation, assisting law enforcement, determining the scope of the breach, and so forth. Notably, it is unclear whether there is an obligation for governmental entities to notify Utah residents when a breach that may involve personal information is discovered.

Amendments to Pennsylvania's Data Breach Law
A number of significant amendments to Pennsylvania's data breach law are set to go into effect on May 3, 2023. Notably, an expanded definition of "personal information" will include medical and health insurance information, and a user name or email address in combination with a password or security questions and answers that would permit access to an online account.[8]

The amendments also modify the point at which a covered entity is required to provide notice of a data breach. [9] Under current law, a breach notification is required following *discovery* of a breach. Once the amended law goes into effect in May, companies will be required to issue a breach notice following a *determination* of a breach.[10] This modification is not merely semantic. The amendments define both "Discovery" and "Determination." "Determination" is "[a] verification or reasonable certainty that a breach of the security of the system has occurred," while "Discovery" is "[t]he knowledge of or reasonable suspicion that a breach of the security of the system has occurred." In shifting from "Discovery" to "Determination," the law does not require companies to notify of a data breach until they are at least reasonably certain a breach has occurred. Notably, Pennsylvania law does not require notification of a data breach to the state attorney general or other government entity, and the recent amendments do not add such a requirement.

Additionally, the amendments impose breach notification requirements on state agencies and their contractors. Upon "discovery" (as now defined) of a breach, a state agency contractor must notify the Chief Information Security Officer (CISO) of the customer state agency "as soon as reasonably practical, but no later than the time period specified in the applicable terms of the contract between the State agency contractor and the State agency…."[11]

Looking Ahead
State data breach laws continue to expand across the country, complicating obligations for companies that collect personal information from individuals nationwide. DWT's Privacy and Security team will continue to monitor these developments.
CLICK HERE.

It's Not Just Illinois Anymore. Biometric Identifier Laws Increase Across US

Biometric identifiers are unique to every individual. They include your fingerprints, facial structure, and even how you walk. There is the Illinois Biometric Information Protection Act ("BIPA"), and biometric protection bills are currently working their ways through the legislatures in Maryland and Mississippi. We now turn to two unique biometric laws that were passed by the New York City Council in 2021 that regulate the collection of customers and renters' biometric data in NYC.

NYC's Biometric Identifier Information Law ("BII"), NYC Admin. Code §§ 22-1201 – 1205, regulates businesses' collection and processing of "biometric identifier information," which is defined as a "physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual." It bars the use of biometric data for transactional purposes to sell, trade, or otherwise profit from the transaction of biometric information. Businesses that utilize biometric information are required to notify patrons of the business' collection of biometric data by posting formal notices near all physical entrances to the business. BII defines biometric identifier information as a physiological or biological characteristic that is used to identify an individual, "including, but not limited to: (i) a retina or iris scan, (ii) a fingerprint or voiceprint, (iii) a scan of hand or face geometry, or any other identifying characteristic." This would include facial recognition systems used by in-store security. The regulation covers "commercial establishments," which include places of entertainment, retail stores, restaurants, and bars. A customer is defined as "a purchaser or lessee, of goods or services from a commercial establishment." Therefore, unlike the BIPA, the BII does not apply to the collection of

employees' biometric data. However, it does prohibit the sale of both customers' and employees' biometric data. The BII provides for a private right of action. The BII also provides for statutory damages of $500 to $5,000 per violation, plus attorney's fees, expert fees, and costs. A business can avoid a suit by providing an express written statement within 30 days of a complaint that the violation has been remedied.

NYC's Tenant Data Privacy Act ("TDPA"), NYC Admin. Code §§ 26-3001 – 3007, prohibits landlords from selling, leasing or otherwise disclosing tenants' data, including biometric data, collected by smart access systems. This includes smart access systems that provide access to buildings, common areas, or individual apartments. A smart access building is defined as one that uses a keyless entry system, including electronic or computerized technology through the use of key fob, RFID cards, mobile apps, biometric information, or other digital technology to grant access to a building or a part of a building. This includes buildings that provide access through facial recognition, fingerprint, or hand scan systems. The TDPA provides an aggrieved tenant with a private right of action. The TDPA allows for the recovery of statutory damages of $200 to $1,000 per tenant, in addition to the recovery of attorney's fees.

Recently, a class action lawsuit was filed against Amazon related to alleged violations of the BII due Amazon's collection of customer palm prints at its Amazon Go stores in NYC. The Amazon Go stores do not have a traditional check-out when a customer purchases items, and instead tracks customers and their purchases as they move through the store, and charges their Amazon accounts when they leave the store. The putative class alleges that Amazon violated the BII because it only recently began posting signs informing their NYC customers that it was using biometric recognition technology despite the fact that the BII has been in effect for over a year. The complaint alleges that in order to make the no check-out process work in their stores that Amazon has to track customers in the store, including scanning the palms of some customers. Amazon states that it does not utilize biometric surveillance to monitor shoppers, but instead other technology to monitor shoppers that does not constitute biometric technology. Amazon states that purchasing via palm scan is only one of various ways customers can complete their purchases, and that all of the privacy disclosure information is provided at the time of enrollment. Because of the lack of a federal data privacy law, states, and even local jurisdictions are beginning to pass their own data privacy laws, like the BII.
CLICK HERE.

California's Pay Transparency Laws

Since 2018, the California Equal Pay Act ("CEPA") has prohibited employers from asking applicants about their salary history, including compensation and benefits, during the hiring process. California also requires employers to provide the pay scale for a position upon reasonable request by an applicant. However, in 2022, California passed SB 1162, which expanded the disclosure requirements imposed on employers, effective January 1, 2023.

Covered Employers
California's disclosure laws apply to employers with 15 or more employees nationwide, and only one employee needs to be physically located in California for the law to apply. Moreover, the Department of Labor Standards Enforcement (DLSE) has interpreted the job posting requirement to apply if the posted position "may ever be filled in California, either in-person or remotely."

If the employer utilizes third parties to "announce, post, publish, or otherwise make known a job posting," the employer must provide the pay scale to the third party that, in turn, must include the pay scale on any job posting.

Disclosure Requirements
In addition to requiring disclosure of pay scale information to applicants, upon request, California employers are now required to include pay scale information in any job posting and provide existing employees with pay scale information for the employee's current position upon request. The DLSE interprets the law to require the pay scale for the position to be included directly within the job posting. In other words, employers cannot require the applicant to go elsewhere to find the pay range.

"Pay scale" means the base salary or hourly wage range or set rate that the employer "reasonably expects" to pay for the position. The DLSE recently clarified that the "pay scale" need not include bonuses, tips, or other benefits. However, piece rate and commission wages must be included in the pay scale information if the job position compensates

employees either in whole or in part based on a task, piece, or commission. In such circumstances, the job posting or disclosure to a current employee must include the piece rate or commission range that the employer "reasonably expects to pay for the position."

Recordkeeping and Penalties
California employers must keep records of wages, wage rates, job classifications, and other terms and conditions of employment for a period of three years. Additionally, starting January 1, 2023, an employer must keep records of a job title and wage rate history for each employee for the duration of the employment plus three years after the end of the employment.

The DLSE can inspect these records to determine if there is a pattern of wage discrepancy.

If an employer violates the disclosure requirements, an employee or applicant who claims to be aggrieved may file a written complaint with the DLSE within one year after the date they learned of the violation. An employee or applicant may also file a civil action for injunctive relief or any other relief that a court deems appropriate.

The DLSE may order employers to pay a civil penalty between $100 and $10,000 per violation. However, employers can avoid the penalty for a first-time violation if the employer demonstrates that all job postings for open positions have been updated to include the required pay scale information.
CLICK HERE.

Colorado's Pay Transparency Laws

Colorado's Equal Pay for Equal Work Act ("EPEWA") requires employers to include compensation and benefits information in all job postings and notifications of promotional opportunities.

Covered Employers
The EPEWA covers all employers, public or private, that employ at least one person in Colorado. Employees of covered employers must also comply with the pay transparency requirements of the EPEWA.

The EPEWA does not apply to employers with no employees in Colorado. If an employer has no employees in Colorado at the time of its hiring or promotion decision, then the requirements of the EPEWA do not apply to the employer for that hiring or promotion decision, even if it considers Colorado applicants, or ultimately hires someone who would work in Colorado.

The EPEWA does not apply to a third-party that shares or re-posts another employer's job. An employer is not liable for violation of the EPEWA if it has a compliant posting, but then a third party, without being hired or instructed by the employer, re-posts the employer's job without the required information.

Covered Job Advertisements
Employers are not required to advertise job openings, or have job postings, except as needed to notify existing employees of promotional opportunities. Compensation and benefits must be disclosed only if an employer chooses to have a job posting. If an employer advertises or posts a job opening, the employer must disclose compensation and benefits information in each posting for each job posted. A job posting includes any electronic or hard copy communication that the employer has any specific job(s) available or is accepting job applications for a particular position.

Employers do not need to disclose compensation and benefits information in job postings for jobs that will be performed entirely outside of Colorado (including non-Colorado jobs that may include modest travel to Colorado), even if the job posting is published in Colorado (or is an online posting that reaches Colorado).

Remote work performable in Colorado or elsewhere for a covered employer must comply with the EPEWA. A remote job posting, even if it states that the employer will not accept Colorado applicants, remains covered by the EPEWA.
Employers do not need to disclose compensation and benefits information in printed or hardcopy job postings that are posted or distributed entirely outside of Colorado. For example, compensation and benefits need not be included in a

printed advertisement or posting entirely in another state, but must be included in an online posting, because online postings are accessible by Colorado residents.

An employer does not need to disclose compensation or benefit information in a help wanted sign or similar communication stating only generally (i.e., without listing specific positions) that an employer is hiring.

Job Advertisement Disclosure Requirements

Employers must include in each job posting (1) the rate of compensation (or a range thereof), including salary and hourly, piece, or day rate compensation; (2) a general description of any bonuses, commissions, or other compensation; and (3) a general description of all benefits the employer is offering for the position.

Benefits that must be generally described include health care, retirement benefits, paid days off, and any tax-reportable benefits, but not minor "perks" like use of an on-site gym or employee discounts. At a minimum, employers must describe the nature of these benefits and what they provide, not specific details or dollar values — such as listing that the job comes with "health insurance," without needing to detail premium costs or coverage specifics. Employers cannot use an open-ended phrase such as "etc.," or "and more," rather than provide the required "general description of all of the benefits."

An employer may post compensation as a range from the lowest to the highest pay it actually believes it might pay for the particular job, depending on circumstances such as employee qualifications, employer finances, or other operational considerations. If the pay might be different inside and outside Colorado, the range should be what the employer would pay in Colorado. A range's bottom and top cannot include open-ended phrases like "$30,000 and up" (with no top of the range), or "up to $60,000" (with no bottom). An employer may ultimately pay more or less than a posted range, as long as the range, at the time of posting, was what the employer genuinely believed it would be willing to pay for the job.

For jobs that earn tips, the Act requires "the hourly or salary compensation" the employer will pay be included in the job posting. A posting does not need to, but may, give an estimated amount of tips, as long as the posting still specifies what the employer itself will pay, aside from any tips.

Electronic postings (e.g., webpages or emails), need not include all required compensation and/or benefits, if they link to such information — as long as the posting makes clear that the link gives access to compensation and benefits for each specific job posted. It is the employer's responsibility to assure continuous compliance with functionality of links, up-to-date information, and information that applies to the specific job posting (e.g., not a single pay "range," or identical benefits, for multiple jobs for which the actual pay ranges or benefits would be different).

Recordkeeping Requirements

For each employee, an employer must keep records of the employee's job description and compensation (including salary or hourly wage, benefits, and all bonuses, commissions, and other compensation received). Records must include any changes to job description or compensation over time.

Employer must maintain these records for the duration of the employee's employment plus two years thereafter. This recordkeeping requirement only applies to employees in Colorado.

If a court finds that an employer failed to comply with record keeping requirements an employee is entitled to a rebuttable presumption that the records contained information favorable to the employee's claim. The employee is also entitled to a jury instruction that the employer's failure to keep records can be considered evidence that the violation was not made in good faith.

Penalties and Fees for Violations

Any person aggrieved by (i.e., witnessed, suffered, or injured by) a perceived violation may file a complaint with the Colorado Department of Labor ("CDOL") within one year of learning of the violation. A person may file an anonymous tip with the CDOL. The CDOL may also initiate its own investigation based on information received without a formal complaint.

If the CDOL determines a violation has occurred, it may issue a fine of $500 to $10,000 for each violation. Failure to include compensation and benefit information in one or more postings for a job is one violation regardless of the number of postings listing that job. The CDOL may waive or reduce particular fines for good cause.

Currently, the CDOL is prioritizing proactive outreach and education over penalties. Accordingly, when it receives a complaint or information about a potential violation it has offered employers an opportunity to cure the violation before it initiates a formal investigation that could result in fines. It is uncertain how long the CDOL will continue the practice of offering an opportunity to cure a violation.

No civil action is available. However, if an employee brings a claim for wage discrimination based on sex and the court finds that the employer violated the EPEWA's pay transparency requirements, then the court may order "appropriate relief."
CLICK HERE.

New York City's Pay Transparency Laws

The salary disclosure law, which went into effect November 1, 2022, makes it an "unlawful discriminatory practice" under the New York City Human Rights Law ("NYCHRL" or "Law") for an employment agency, employer, employee or agent to advertise a job opening, promotion or transfer opportunity, in NYC, without providing the position's minimum and maximum annual salary or hourly wage.

Covered Employers and Advertisements

As with other provisions of NYCHRL, "covered employers" are those with at least four employees if one employee is in NYC (or one or more domestic workers), and employment agencies regardless of their size. For purposes of counting employees, employers are required to include full-time and part-time employees, paid interns, domestic workers, owners, family members who are employees, independent contractors working in furtherance of any employer's business enterprise, and any other category of worker protected by the NYCHRL.

Any written description regarding an available job, promotion, or transfer opportunity that is publicized internally or externally and could be performed, in whole or part, in NYC, either at the employer's location, at an alternate work location, or at a remote location selected by the employee, must comply with the pay transparency law. Some examples of job advertisements that are covered by the Law are:

- Postings on internal bulletin boards;
- Internet advertisements;
- Printed flyers distributed at job fairs; and
- Newspaper advertisements.

Employers and Advertisements Not Covered

The Law does not apply to temporary positions at a temporary staffing firm ("staffing agency") as they are already required to provide wage information in compliance with the New York State Wage Theft Prevention Act. A staffing agency is a company who recruits, hires and assigns their staff to other employers to support or supplement their workforce or assist in a special project. While staffing agencies are excluded, covered employers who work with these agencies are not. Employers are not prohibited from hiring, promoting or transferring an employee without using an advertisement. Therefore, the Law does not apply to employers who choose to hire, promote or offer a transfer opportunity without a "written" description.

Disclosure Requirements in Job Advertisements

An employer is required to include the minimum and maximum "annual salary or hourly wage" for jobs, promotions, or transfer opportunities based on the employer's good faith belief of what the employer would pay a successful job applicant, at the time the job advertisement is posted. Notably, the New York City Commission on Human Rights ("NYCCHR") does not interpret the "salary" disclosure requirement to include other forms of compensation or benefits such as tips, bonuses, stocks, overtime pay, severance pay, paid time off, health benefits, employer contributions to retirement or savings plans, or value of employer-provided meals or lodging.

Penalties and Fees for Violations

The NYCCHR is authorized to investigate complaints by the public or initiate its own investigation into violations of

the Law. In addition, current employees can file a lawsuit against their current employer in court.

Violators could be forced to pay monetary damages to the affected employee and a civil penalty of up to $125,000 (or up to $250,000 upon a finding that employer's actions were willful, wanton or malicious). However, first time violators can have their civil penalty reduced to $0 if they submit proof, electronically or in person, that the alleged violation was cured within 30 days of service of a complaint by the NYCCHR. The submission of proof of a cure is "deemed an admission of liability for all purposes" including for use on a subsequent violation to prove willful, wanton or malicious conduct.

In addition, a covered employer who is found to have violated the NYCHRL may be required to amend the offending advertisement, create or update employment policies, conduct trainings, provide notices of rights to covered employee or applicants, and engage in other forms of remedial relief.

Key Differences of New York State and New York City Transparency Laws

New York State's pay transparency law explicitly provides that it does not supersede or preempt local laws or regulations. New York City employers will need to comply with both NYS and NYC laws. While there are many similarities, NYS's law differs in that it does not apply to advertisements for independent contractors or interns; requires a job description, if one exists, in the advertisement; and provides no private right of action for current employees against their current employers.
CLICK HERE.

Pay Disclosure and Transparency Efforts Across the Country

As pay equity and transparency continues to trend in the news, states and localities have passed pay disclosure and transparency laws to further assist employees in evaluating whether they are being paid fairly. These laws vary in scope – some require the disclosure of pay ranges on job postings, others require employers to provide the pay scale for a position upon an applicant or employee's request, and others require employers to automatically provide pay scale information at the time of hire. Despite their differences, all of these pay disclosure laws are aimed at adding transparency to conversations about pay.

At least thirteen jurisdictions have enacted pay disclosure or transparency laws, each with unique requirements for employer compliance:

California: Employers must provide a position's pay scale to applicants and employees upon request. Employers with 15 or more employees must include a position's pay scale in job postings.

Colorado: All employers must disclose in each job posting the hourly or salary compensation, or a range of the compensation, and a general description of all of the benefits and other compensation to be offered to the applicant.

Connecticut: All employers must provide a position's wage range at the earliest of either the applicant's request or at the time of making the applicant an offer of compensation. Employers must also provide applicants and employees with the wage range for their position upon hiring, a change in position with the employers, or their first request for a wage range.

Illinois: Current employees may request anonymized data for the pay rates of employees in their job title *or job classification, limited to their employer and limited to the county where the employee works.*

Maryland: All employers must provide applicants, upon request, with the wage range for the position for which they are applying.

Nevada: All employers must provide a position's wage or salary range or rate to an applicant who interviews for the position. Employers also must provide current employees with the wage or salary range or rate for a promotion or transfer to a new position if the employee applies for the promotion or transfer, interviews for or is offered the promotion or transfer, and requests that range or rate.

New Jersey

- Jersey City, New Jersey: Employers with 5 or more employees must disclose in each job posting the minimum and maximum salary range and benefits.

New York: Employers with 4 or more employees must disclose in each job posting the pay range that the employer in good faith believes to be accurate for that position at the time of posting. See our prior post regarding New York here.

- Albany County, New York: Employers must disclose in each job posting the minimum and maximum salary or hourly wage for such position
- Ithaca, New York: Employers with 4 or more employees must disclose in each job posting the minimum and maximum hourly or salary compensation.
- New York City, New York: Employers with 4 or more employees must disclose in each job posting the minimum and maximum hourly or salary compensation.
- Westchester County, New York: Employers with 4 or more employees must disclose in each job posting the minimum and maximum salary.

Ohio

- Cincinnati, Ohio: Employers with 15 or more employees must provide the pay scale to applicants who make a reasonable request after receiving a conditional offer of employment.
- Toledo, Ohio: Employers with 15 or more employees must provide the pay scale to applicants who *make a reasonable request after receiving a conditional offer of employment.*

Rhode Island: All employers must provide applicants, upon request, with the wage range for the position for which they are applying. If the applicant does not request the wage range, employers should provide it prior to discussing compensation. Employers must provide current employees, upon request, the wage range for their position at any time during their employment.

Washington: After a conditional offer of employment is made, employers with 15 employees or more must provide the minimum wage or salary for a position to applicants who request it. Employers must disclose wage or salary ranges to current employees, upon request, who have been offered a new position or promotion. Employers must disclose in each job posting the opening wage scale or salary range, and a general description of all benefits and other compensation to be offered. We anticipate that more states and localities will pass pay disclosure and transparency laws as employees continue to demand more information related to pay equity. Accordingly, employers should continue to monitor pay disclosure and transparency legislation in states where they operate. Moreover, employers should consider conducting privileged pay equity analyses to ensure compliance, understand risks, and investigate and mitigate potential disparities.
CLICK HERE.

New York City Adopts Final Rules on Automated Decision-making Tools, AI in Hiring

On April 6, 2023, the New York City Department of Consumer and Worker Protection (DCWP) adopted highly anticipated final rules implementing the city's law regulating the use of automated employment decision tools (AEDT) tools in hiring that will take effect on July 5, 2023.

The AEDT law, which took effect on January 1, 2023, restricts the use of automated employment decision tools and artificial intelligence (AI) by employers and employment agencies by requiring that such tools be subjected to bias audits and requiring employers and employment agencies to notify employees and job candidates that such tools are being used to evaluate them.

The final rules come after the DCWP first proposed rules in September 2022, which it later revised in December 2022 after a public hearing. The final rules include a number of changes to earlier versions, including expanding the scope of "machine learning, statistical modeling, data analytics, or artificial intelligence," modifying bias audit standards, and clarifying information that must be disclosed. Here are some key points from the new rules.

Automated Employment Decision Tools
The law defines AEDT as "any computational process, derived from machine learning, statistical modeling, data analytics, or artificial intelligence, that issues simplified output, including a score, classification, or recommendation"

that is used to "substantially assist or replace discretionary decision making for making employment decisions that impact natural persons." Maintaining the approach adopted in the in the December 2022 revised proposed rules, the final rules provide that the phrase "to substantially assist or replace discretionary decision making" refers to:

- relying "solely on a simplified output (score, tag, classification, ranking, etc.), with no other factors considered;" or
- using a simplified output as "one of a set of criteria" where it is weighed more than others in the set; or
- using a simplified output to "overrule" other conclusions based on other factors, including "human decision-making."

On the other hand, the final rules alter the definition of "machine learning, statistical modeling, data analytics, or artificial intelligence" proposed in the earlier versions of the rules, and provide that the term means "a group of mathematical, computer-based techniques" that: (i) "generate a prediction, meaning an expected outcome" or "that generate a classification, meaning an assignment of an observation to a group" and "for which a computer at least in part identifies the inputs, the relative importance placed on those inputs, and, if applicable, other parameters for the models in order to improve the accuracy of the prediction or classification." This definition omits techniques "for which the inputs and parameters are refined through cross-validation or by using training and testing data," which had been included in the earlier versions of the proposed rules.

Bias Audits

Under the AEDT law, before employers or employment agencies may use AEDTs, the tools must be subjected to "a bias audit conducted no more than one year prior to the use of such tool." A "bias audit" is defined as "an impartial evaluation by an independent auditor" to assess the tool's potential "disparate impact" on sex, race, and ethnicity. The employer or employment agency must also post a "summary of the results of the most recent bias audit" on its website. The final rules clarify the requisite calculations for a bias audit. Where an AEDT is used to select candidates for hiring or promotion to move forward in the hiring process or classifies them in groups, "a bias audit must, at a minimum":

1. "Calculate the selection rate for each category";
2. "Calculate the impact ratio for each category";
3. Separately calculate the impact on: (i) "[s]ex categories"; (ii) "[r]ace/[e]thnicity categories"; and (iii) "intersectional categories of sex, ethnicity, and race (e.g., impact ratio for selection of Hispanic or Latino male candidates vs. Not Hispanic or Latino Black or African American female candidates)."
4. Ensure that all the calculations are "performed for each group, if an AEDT classifies candidates for employment or employees being considered for promotion into specified groups (e.g., leadership styles)"; and
5. "Indicate the number of individuals the AEDT assessed that are not included in the required calculations because they fall within an unknown category."

The final component represents an additional requirement that was not expressly addressed in the prior versions of the rules.

In another change to the bias audit requirements from the earlier versions of the proposed rules, the final rules state that notwithstanding the requirements of paragraphs 2 and 3, detailed above (and the similar requirements for a bias audit on an AEDT that scores candidates for employment or employees being considered for promotion), "an independent auditor may exclude a category that represents less than 2% of the data being used for the bias audit from the required calculations for impact ratio." The final rules also specify that "[w]here such a category is excluded, the summary of rules must include the independent auditor's justification for the exclusion, as well as the number of applicants and scoring rate or selection rate for the excluded category."

Sources of Data

The final rules incorporate provisions that address the use of historical data and test data. The provisions relating to the use of historical data are largely unchanged. According to the final rules, multiple employers or employment agencies using the same AEDT may rely on the same bias audit conducted using historical data of other employers or employment agencies only if the employer or employment agency "provided historical data from its own use of the AEDT to the independent auditor conducting the bias audit or if such employer or employment agency has never used the AEDT."
The final rules relating to the use of test data are more explicit about the limited circumstances in which an employer or employment agency may utilize test data, and specify that the bias audit may rely upon "test data if insufficient

historical data is available to conduct a statistically significant bias audit." The final rules maintain the requirement that the summary of results for a bias audit that uses test data "must explain why historical data was not used and describe how the test data used was generated and obtained."

Characteristics of an Independent Auditor

The final rules end any lingering uncertainty about individuals or entities who can perform the bias audit required by the law by retaining the definitions of an independent auditor contained in the December 2022 proposed rules. As such, the final rules provide that an "[i]ndependent auditor" means "a person or group that is capable of exercising objective and impartial judgment on all issues within the scope of a bias audit of an AEDT." The final rules identify three disqualifying characteristics, namely a person or group that:

i. "is or was involving in using, developing, or distributing the AEDT;
ii. at any point during the bias audit, has an employment relationship with an employer or employment agency that seeks to use or continue to use the AEDT or with a vendor that developed or distributes the AEDT; or
iii. at any point during the bias audit, has a direct financial interest or a material indirect financial interest in an employer or employment agency that seeks to use or continue to use the AEDT or in a vendor that developed or distributed the AEDT."

Bias Audit Summary Results

Before using an AEDT, employers and employment agencies must publicly disclose the date of the most recent bias audit of the AEDT and a "summary of the results." The final rules expand the December 2022 list of information that must be included in the summary, and specifies that it must include:

- "the source and explanation of the data used to conduct the bias audit";
- "the number of individuals the AEDT assessed that fall within an unknown category"; and
- "the number of applicants or candidates, the selection or scoring rates, as applicable, and the impact ratios for all categories;" and
- "[t]he distribution date of the AEDT.

The final version of the rules continue to specify that the notice requirements may be met "with an active hyperlink to a website" that must be "clearly identified as a link to the results of the bias audit." Additionally, the summary must be posted "at least [six] months after its latest use of the AEDT for an employment decision."

The final rules also specify the required notices to candidates and employees. These provisions are unchanged from the December 2022 proposed rules, and specify that notice to candidates may be provided via the website, or in a job posting or by mail "at least 10 business days before use of an AEDT." Notice to employees being considered for promotion made be provided in a policy or procedure that is distributed "at least 10 business days before use of an AEDT."

Key Takeaways

Employers are increasingly relying on AEDTs and AI systems to make hiring decisions or screen candidates, which can increase efficiency and improve results. New York City is one of several jurisdictions to put guardrails around this emerging technology amid concerns with bias. The newly adopted final rules by the New York City DCWP provide further guidance and clarification on the city's new restrictions.

Employers and employment agencies in New York City may want to consider reviewing their use of automated decision-making tools or AI in making hiring and promotion decisions. If such tools are being used or are planned to be used, employers may want to consider whether the tools being considered have been subjected to bias audits.
CLICK HERE.

Reminder for Illinois (and other) Employers: Restrictions Apply When Using Artificial Intelligence Analysis During the Hiring Process

Illinois and other jurisdictions have adopted, or are considering, laws establishing parameters for employer use of AI during the hiring process.

The current attention being given to ChatGPT and other technologies using artificial intelligence (AI) is prompting companies to consider (or take another look) at how AI can and/or should play a role in their operations. From an

employment law perspective, employers in Illinois – and elsewhere – should be aware of existing laws and guidance, and also should keep an eye out for the additional restrictions that will undoubtedly come as the use of AI becomes more prevalent.

In 2020, Illinois adopted the Artificial Intelligence Video Interview Act (820 ILCS 42/1), which establishes parameters for employer use of AI during the hiring process. If an employer intends to ask applicants to record video interviews so that it can use an AI analysis of such videos as part of the evaluation process, the employer must:

- Notify each applicant before the interview that AI may be used to analyze the interview and consider the applicant's fitness for the position;
- Provide each applicant with information before the interview explaining how the AI works and what general types of characteristics it uses to evaluate applicants; and
- Obtain the applicant's consent for the use of AI to evaluate the interview. Where consent is not obtained, AI may not be used to evaluate the applicant.

Sharing of such videos is limited to those with the expertise or technology necessary to evaluate the applicant's fitness for a position. The videos (including all copies) must be destroyed within 30 days of a request by the applicant. These restrictions presumably apply to both new hires and employees who are seeking new positions within a company.

Illinois is not the only jurisdiction with AI restrictions on the books or under consideration. Bryan Cave Leighton Paisner's Data Privacy group has prepared a summary of current and pending AI legislation around the United States. California is among the jurisdictions currently reviewing proposed laws and regulations on the subject of the use of AI when making employment decisions, while Maryland enacted a law similar to Illinois' in 2020, placing restrictions on the use of facial recognition services during pre-employment interviews until the applicant provides consent.

A more extensive law will be enforced in New York City beginning July 5, 2023: The New York City Automated Employment Decision Tools Law ("AEDTL") which, among other things, requires employers to (a) conduct an audit for potential bias before using any artificial intelligence tools that screen candidates for hire or promotion, (b) give advance notice to candidates concerning the use of such tools, and (c) provide information on their websites about the tools and data collected. More information on the AEDTL is available here.

The potential for bias in the use of artificial intelligence tools is a key concern of the federal Equal Employment Opportunity Commission (EEOC) as well. The EEOC launched an agency-wide initiative on the subject in 2021, with a goal of ensuring that, "the use of software, including artificial intelligence (AI), machine learning, and other emerging technologies used in hiring and other employment decisions comply with the federal civil rights laws that the EEOC enforces."

In May 2022, the EEOC issued guidance on the subject of, "The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees." This guidance provides definitions of key terms and explains how the use of algorithmic decision-making tools may violate the Americans with Disabilities Act (ADA), and notes that the use of a third-party vendor to develop and/or administer such a tool is not likely to insulate the employer from liability in connection with the results of using that tool. The EEOC held a public hearing on the issue of employment discrimination and the use of AI in January 2023, and is likely to continue its focus on this developing area. As the use of AI in the hiring and selection process continues to evolve, employers should: (1) become familiar with artificial intelligence concepts; (2) examine, understand, be able to explain, and monitor their automated recruiting tools and practices; and (3) take steps to avoid bias and comply with applicable law.
CLICK HERE.

5 Things Kentucky Employers Need to Know About the State's New Medical Cannabis Law

Kentucky just became the 38th state to legalize medicinal cannabis when Governor Andy Beshear signed SB 47 into law on March 31. This comes after many years of failed legislation and just a few months after the governor signed an executive order allowing Kentuckians diagnosed with certain medical conditions and receiving palliative care to purchase, possess, and use cannabis. While the new law legalizes medicinal use, you should note that its reach is limited. For example, the qualifying medical conditions are not expansive, and the law provides for strict regulation of the industry by the Cabinet for Health and Family Services. Moreover, the law not set to take effect until January 1, 2025

– but you should prepare now to field questions from your employees and assess the new law's potential impact on your workplace policies and practices. Here are the answers to five top questions employers are asking.

1. Who Does the Law Protect?

The law is set to provide access to medicinal cannabis only for those individuals with a qualifying medical condition. These include:

- any type or form of cancer, regardless of stage;
- chronic, severe, intractable, or debilitating pain;
- epilepsy or any other intractable seizure disorder;
- multiple sclerosis, muscle spasms, or spasticity;
- chronic nausea or cyclical vomiting syndrome resistant to other conventional medical treatments; and
- post-traumatic stress disorder.

While the number of qualifying conditions is relatively low, the law also allows the Kentucky Center for Cannabis to identify other medical conditions or diseases for which scientific data and evidence demonstrates that cannabis is likely to have medical, therapeutic, or palliative benefits.

Those who qualify will have to register with the Cabinet for Health and Family Services as a qualified registered cardholder and will be issued a registry identification card.

The law will also protect and regulate medicinal cannabis businesses in the Commonwealth, including cultivators, dispensaries, producers, and safety compliance facilities. These businesses must obtain a license from the Cabinet for Health and Family Services and will be subject to inspection and investigation by the Cabinet for compliance with the law.

2. Are Employees Governed by Professional Licensing Boards Subject to Disciplinary Action for Use of Medicinal Cannabis?

Generally, an employee who holds a professional license from a state licensing board will not be subject to disciplinary action if they are a registered qualified patient and they do not possess more medicinal cannabis then permitted by the law.

However, certain employees licensed under the Kentucky Board of Nursing, the Kentucky Board of Podiatry, or the Kentucky Board of Medical Licensure, may be subject to disciplinary action if there is probable cause to believe that they have become impaired by or abused medicinal cannabis. They may also be subject to discipline by their licensing board if their use interferes with their professional, social, or economic functions in the community or causes a loss of self-control.

However, the potential for disciplinary action by a licensing board does not stop with just medical professionals. The law will not protect any employee who undertakes a task when under the influence if doing so would constitute negligence or professional malpractice.

3. Are Employers Required to Permit Employees to Use Medicinal Cannabis?

Employees may believe that the new law will protect them from adverse employment actions if they are qualified and registered to use medicinal cannabis within the state. However, Kentucky the law allows employers to limit or prohibit use even by qualified, registered employees in the workplace. Here are a few points to note about the new law:

- Employment Policies. Employers are not required to permit or accommodate the use, consumption, possession, transfer, display, transportation, distribution, sale, or growing of medicinal cannabis in the workplace. Employers may include provisions in their employment contracts prohibiting use by employees. Additionally, they may create or rely upon existing personnel policies prohibiting the use of cannabis – including medicinal use – by employees.
- Operating Equipment. Employers may prohibit employees from using equipment, machinery, or power tools if you believe the employee's medicinal cannabis use poses an unreasonable safety risk. In fact, the operation of some equipment, such as vehicles, aircraft, or other vessels, while under the influence would not only be a potential violation of employment policies, but the law as well. While the new law

legalizes the use of medicinal cannabis, it does not de-criminalize the operation of a vehicle while under the influence or consumption while operating those vehicles.

- Restrictions on Certain Properties. Employees that work at any preschool, primary, or secondary school; any correctional facility; or on federal government property will also be legally restricted from the use or possession of medicinal cannabis while working in these environments.
- No New Protected Class. The law does not create a new protected class of individuals or give employees the right to bring a claim against an employer for wrongful discharge or discrimination for using medicinal cannabis.

4. Are Employers Required to Make Reasonable Accommodations?

While the medical conditions outlined in the new law may qualify as a disability under the Americans with Disabilities Act (ADA) and may require employers to reasonably accommodate that disability, they do not require employers to accommodate those disabilities by permitting the use of medicinal cannabis in the workplace.

It is important to note that cannabis use is still illegal under federal law. In fact, the ADA (which applies to businesses with 15 or more employees) provides that a "qualified individual with a disability" shall **not** include any employee or applicant who is currently engaged in the illegal use of drugs, when the covered employer acts on the basis of such use. Another subsection provides that a covered employer may (1) prohibit the illegal use of drugs and the use of alcohol at the workplace by all employees; and (2) required that employees shall not be under the influence of alcohol or be engaging in the illegal use of drugs at the workplace.

5. Can Employers Still Test for Drug Use?

Yes. Consistent with the ADA and the new Kentucky law, employers in the state may continue to test employees for medicinal cannabis and act based on a positive result.

Under the ADA, a test to determine the illegal use of drugs is not considered a medical examination. The ADA also states, "nothing in this subchapter shall be construed to encourage, prohibit, or authorize the conducting of drug testing for the illegal use of drugs by job applicants or employees or making employment decisions based on such test results." The new Kentucky law permits employers to establish and enforce drug testing policies, drug-free workplace policies, and zero-tolerance drug policies. In addition, the law explicitly allows employers to drug test cardholding employees that the employer believes, in good faith, to be impaired. These good faith determinations of impairment should include a behavioral assessment of impairment and testing for the presence of cannabis by established methods. If the behavioral assessment and testing demonstrate impairment on the part of the cardholding employee, that employee may attempt to refute the employer's findings.

Any employee that is discharged for consuming medicinal cannabis in the workplace, working while under the influence, or testing positive for a controlled substance will not be eligible for unemployment insurance benefits if those actions violate their employment contract or established personnel policies.

Next Steps

Things will not change overnight in Kentucky, especially given the new law's January 1, 2025, effective date. However, Kentucky employers should prepare by taking the following actions:

- Review current drug use and testing policies with your human resources department to discern whether any changes need to be made to policies prior to the act's effective date.
- Watch for administrative regulations, which will likely be issued prior to the effective date and may further clarify your responsibilities as they relate to employees who are qualified and registered to use medicinal cannabis.

CLICK HERE.

Michigan Extends Employment Law Protections to Prohibit Discrimination Based on Sexual Orientation and Gender Identity

Although many company equal employment opportunity and no-harassment policies prohibit discrimination or harassment based on sexual orientation and gender identity, not all applicable state civil rights laws provide such protections. Currently, twenty-two states, the District of Columbia, and a number of localities have laws prohibiting discrimination in employment based on sexual orientation and gender identity.

Last month, Michigan joined this group of states by expanding its civil rights statute (known as the Elliott-Larsen Civil Rights Act) to expressly cover sexual orientation and gender identity and expression. Michigan's Democratic-led House and Senate, joined by several Republicans, voted for the legislation, which covers employment, housing, and other areas. In signing the legislation, Governor Gretchen Whitmer stated that, "we are taking a long overdue step to ensure that no one can be fired from their job or evicted from their home because of who they are or how they identify."

As we previously reported, the U.S. Supreme Court held in 2020 that Title VII of the Civil Rights Act of 1964 prohibits discrimination against individuals based on sexual orientation and gender identity, expanding federal protections to all U.S. employees for the first time. Although already prohibited by federal law, Michigan considered it important that its civil rights statute similarly provide protections against discrimination based on sexual orientation and gender identity and provide aggrieved individuals with recourse under state law.

Many Michigan employer policies have long prohibited discrimination and harassment against employees and applicants for employment based on sexual orientation and gender identity. However, in light of the above changes in Michigan law, Michigan employers should nonetheless review their policies and procedures, as well as training materials, to ensure that they are appropriately updated to comply with Michigan as well as federal law.
CLICK HERE.

Columbus, Ohio, Bans Inquiries Into Applicants' Salary History

The City of Columbus joins Toledo and Cincinnati as the latest Ohio city to prohibit employers from asking prospective employees about past compensation.

Effective March 1, 2024, employers operating in Columbus may not ask about a prospective employee's wage or salary history.

What is Covered?

The new ordinance makes it an "unlawful discriminatory practice" for an employer to:

1. Ask about an applicant's salary history, which includes current or prior wages, benefits, or other compensation. Salary history does not include any objective measure of the applicant's productivity, such as revenue, sales, or other production reports.
2. Screen job applicants based on their current or prior wages, benefits, or other compensation.
3. Rely solely on the applicant's salary history in deciding whether to offer employment or in determining wages, benefits, or other compensation for the applicant.
4. Refuse to hire or otherwise disfavor, injure, or retaliate against an applicant for not disclosing salary history to an employer.

Employers may still discuss with applicants expectations as to salary, benefits, and other compensation.
Unlike Toledo and Cincinnati, Columbus does not require employers to share the pay scale for the position with applicants after a conditional offer of employment.

Who is Covered?

The new ordinance applies to all employers located within the City of Columbus that have at least 15 employees within the city. Covered employers include job placement and referral agencies and other employment agencies that operate on behalf of an entity that otherwise meets the definition of an "employer" under the ordinance.

An "applicant" is any person applying for employment within the geographic boundaries of the City of Columbus and whose application "in whole or in part, will be solicited, received, processed, or considered in the City of Columbus."

Exceptions

The Columbus ordinance does not apply to:

- Any actions taken by an employer under any federal, state, or local law that specifically authorizes reliance on salary history to determine an employee's compensation;
- Applicants for internal transfer or promotion with their current employer;
- A voluntary and unprompted disclosure of salary history information by an applicant;
- Any attempt by an employer to verify an applicant's disclosure of non-salary-related information or conduct a background check, provided that, if such verification or background check discloses the applicant's salary history, such disclosure must not be solely relied on in determining the salary, benefits, or other compensation of such applicant during the hiring process, including the negotiation of a contract;
- Applicants who are re-hired by the employer within three years of the applicant's most recent date of termination of employment by the employer, as long as the employer already has past salary history data about the applicant from their previous employment;
- Employee positions for which salary, benefits, or other compensation are determined by procedures established by collective bargaining; and
- Federal, state, and local governmental employers, other than the City of Columbus.

Civil Penalties

The ordinance gives applicants the right to file an administrative complaint with the Columbus Community Relations Commission. Employers that violate the ordinance could face civil fines of up to $5,000, dependent on number of offenses.

Next Steps for Employers

The ban on salary history inquiries continues to creep across the state and country. Even in jurisdictions that allow such inquiries, there are risks for employers. With remote workers and expanded geographical footprints, companies need to stay abreast of the changing laws on pay transparency and pay equity.

Beyond salary history bans, states like California, Colorado, New York, and Washington, and a handful of cities require pay information to be disclosed in job postings.
CLICK HERE.

Indiana Likely to Become Seventh State to Enact a Comprehensive State Privacy Law

On April 13, 2023, the Indiana Senate concurred to the Indiana House's amendments of Senate Bill 5 ("SB 5") a day after the House returned the bill to the Senate with amendments, and a couple days after the Indiana House unanimously voted to approve SB 5. SB 5 now will head to Governor Eric Holcomb for a final signature, where he will have seven days upon transmission to sign SB 5 into law or veto it. This could make Indiana the seventh U.S. state to enact comprehensive privacy legislation.

Applicability

SB 5 would apply to a person that conducts business in Indiana or produces products or services that are targeted to residents of Indiana and that during a calendar year: (1) controls or processes personal data of at least one hundred thousand (100,000) consumers who are Indiana residents; or (2) controls or processes personal data of at least twenty-five thousand (25,000) consumers who are Indiana residents and derive more than fifty percent (50%) of gross revenue from the sale of personal data.

SB 5's protections would apply to residents of Indiana who act for a personal, family or household purpose, with express exemption for individuals acting in a commercial or employment context. The bill also contains a number of exemptions, including exceptions for financial institutions, affiliates, and data subject to Title V of the Gramm-Leach-Bliley Act, covered entities and business associates under the Health Insurance Portability and Accountability Act of 1996, nonprofit organizations and institutions of higher education.

Controller Obligations
Similar to the other comprehensive state privacy laws, SB 5 would require controllers to limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. In addition, controllers will need consumer's consent to process sensitive data or to process personal data for purposes that are neither reasonably necessary for nor compatible with the disclosed purposes for which the personal data is processed. SB 5 also requires controllers to establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data.
Controllers will need to provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes: (1) the categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights under the law, including how a consumer may appeal a controller's decision with regard to the consumer's request; (4) the categories of personal data that the controller shares with third parties, if any; and (5) the categories of third parties, if any, with whom the controller shares personal data.
SB 5 also will require controllers to conduct and document a data protection impact assessment for each of the following processing activities involving personal data: (1) the processing of personal data for purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for purposes of profiling, if such profiling presents certain reasonably foreseeable risks; (4) the processing of sensitive data; and (5) any processing activities involving personal data that present a heightened risk of harm to consumers.

Consumer Rights
SB 5 provides consumers with the following rights: (1) to confirm whether or not a controller is processing the consumer's personal data and to access such personal data; (2) to correct inaccuracies in the consumer's personal data that the consumer previously provided to a controller; (3) to delete personal data provided by or obtained about a consumer; (4) to obtain either a copy of or a representative summary of the consumer's personal data that the consumer previously provided to the controller in a portable and readily usable format that allows the consumer to transmit the data or summary to another controller without hindrance; and (5) to opt out of the processing of the consumer's personal data for purposes of (A) targeted advertising, (B) the sale of personal data, or (C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

Controllers would have 45 days to respond to consumer rights requests, with a potential 45-day extension in certain circumstances.

Enforcement
SB 5 does not contain a private right of action and would be enforced exclusively by the Indiana Attorney General. The bill provides a 30-day cure period for violations where a company must (1) cure a potential violation, and (2) provide the Attorney General with express written statement that the alleged violation has been cured and actions will be taken to ensure no further violations will occur. In the case a violation is not cured, the Attorney General may initiate an action and may seek an injunction to restrain any violations of the law and a civil penalty up to $7,500 for each violation under the law.

Effective Date
If passed as law, SB 5 will take effect on January 1, 2026.
CLICK HERE.

Montana Legislature Passes Consumer Data Privacy Bill

On April 21, 2023, the Montana legislature unanimously passed Republican Senator Daniel Zolnikov's SB 384. In doing so, Montana became the first Republican-controlled legislature to pass a consumer privacy bill with provisions that closely align with last year's Connecticut Data Privacy Act (CTDPA). As a result, Montana joins California, Colorado, and Connecticut as states with the strongest consumer data privacy bills passed to date. In a first, the Montana bill lowers the traditional 100,000 consumer threshold to 50,000 to presumably take into account Montana's smaller population.

Pending any remaining procedural formalities, the bill will be sent to Montana Governor Greg Gianforte in the coming days. Governor Gianforte can sign the bill, veto it, or allow it become law without his signature.

In the below post, we provide a summary of some of the bill's more notable provisions. Click here for a more detailed

comparison of the Montana bill against the seven bills passed to date.

Lower Applicability Threshold Based on State Population
In a unique provision, the Montana bill applies to persons that conduct business in Montana or that produce products or services that are targeted to Montana residents and that control or process the personal data of not less than 50,000 state residents, excluding personal data controlled or processed solely for purposes of completing a payment transaction. The 50,000-consumer threshold was lowered from 100,000 in a House committee amendment.

The lower threshold presumably was done because of Montana's smaller population in comparison to the populations of other states that have passed bills. Montana's population is approximately 1.1 million. Therefore, a 100,000-consumer threshold would have been approximately 9% of the state's population, which is a much higher percentage than in other states.

Requirement to Recognize Universal Opt-Out Mechanisms
Montana is the first Republican-controlled legislature to pass a bill requiring controllers to recognize universal opt-out mechanisms to effectuate requests to opt-out of sales and for targeted advertising. The Montana bill aligns with the Connecticut law and will not require the Montana Attorney General's office to engage in rulemaking such as occurred in Colorado this past year. This provision will go into effect on January 1, 2025.

Additional Children's Privacy Protections
Montana's bill provides additional privacy protections for children between the ages of 13 and 15. Controllers cannot process the personal data of a consumer for the purposes of targeted advertising or sell the consumer's personal data without the consumer's consent under circumstances in which a controller has actual knowledge that the consumer is at least 13 years of age but younger than 16 years of age. The California and Connecticut laws have similar provisions.

Broad Privacy Rights
The Montana bill aligns with the privacy rights provided in the CTDPA. Consequently, Montana becomes only the second state (after Connecticut) to statutorily provide its residents with the right to revoke their consent (Colorado did so through rulemaking). Montana's bill also allows a state resident to request that a controller delete all personal data that the controller possesses about the consumer as opposed to just personal data that the controller collected directly from the consumer.

The Montana bill also does not require opt-out requests to be verified. In other words, a Montana resident will not have to prove their identity to opt out of the sale of their personal data, for targeted advertising, or for certain types of profiling. Only California and Connecticut have similar provisions.

Sunset on Right to Cure
The Montana bill is enforceable only by the state Attorney General's office. It does not provide a private right of action. The Montana bill requires the Attorney General's office to provide a notice of violation and opportunity to cure; however, the right to cure sunsets on April 1, 2026. Montana is the first Republican-controlled legislature to pass a privacy bill with a sunsetting right to cure.

Effective Date
If signed by the Governor, the Montana law will go into effect on October 1, 2024. That is fourteen months before the January 1, 2026, effective date for the Indiana bill passed earlier this month and three months before the January 1, 2025, effective date for the Iowa bill passed in March.
CLICK HERE.

Washington Legislature Passes My Health My Data Act

Keypoint: With a private right of action, broad applicability to businesses of all sizes and types, a scope that is broader than its name suggests, and strong consent-based requirements and privacy rights, the Washington My Health My Data Act will be a transformative privacy law for the United States.

On April 17, 2023, the Washington legislature passed the My Health My Data Act (MHMD) (HB 1155). The bill now heads to the Washington Governor who can sign it, veto it, or allow the bill to become law without signature.
We have been tracking MHMD since it was first introduced in early January, provided a detailed analysis of the bill after it first passed the House in mid-March, and discussed its definition of "consumer health data" and private right of action in our April 10 weekly post. In the below post, we add to our analysis by providing five key takeaways about MHMD.

1. Enforcement – Private Right of Action
For years, Washington has tried to pass privacy legislation only to have it repeatedly fail on the issue of enforcement. For example, in March 2020, we saw the Washington Privacy Act fail (for a second time) on the issue of including a private right of action.

MHMD broke through this deadlock and will be enforceable both by the Washington Attorney General's office and through a private right of action via the Washington Consumer Protection Act. We will have a deep dive analysis into the contours of the private right of action in an upcoming article. For now, it is enough to note that the inclusion of a private right of action significantly expands the risk companies face when complying with law.

2. Broad Applicability to Businesses
The emerging state privacy law model has used thresholds for applicability based on revenue (e.g., $25 million annual gross revenue), number of consumers' data processed (e.g., process or control personal data of 100,000 consumers), and/or status as a data broker (e.g., control or process personal data of at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data).

In comparison, MHMD applies to "regulated entities," which is defined as any legal entity that: "(a) conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; and (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data." The definition excludes government agencies, tribal nations, or contracted service providers when processing consumer health data on behalf of the government agency.

Rather than basing its applicability on the traditional thresholds, MHMD creates a category of entities called "small businesses" which are regulated entities that (a) collect, process, sell, or share consumer health data of fewer than 100,000 consumers during a calendar year and/or (b) derive less than 50% of gross revenue from the collection, processing, selling, or sharing of consumer health data, and control, process, sell, or share consumer health data of fewer than 25,000 consumers. However, the impact of qualifying as a small business is only a three month delayed effective date as compared to regulated entities.

In addition, while Section 12 provides a number of exemptions, those exemptions are limited to data level, not entity level, exemptions. For example, MHMD contains a CCPA-like data level exemption for personal information subject to the Gramm-Leach-Bliley Act. (The fact that financial institutions do not have an entity level exemption is perhaps indicative of the overall intended breadth of the bill.) Section 12 of MHMD does contain a number of healthcare-related exemptions based on existing health data laws, which is consistent with MHMD's stated purpose to extend protections for health data not covered by those laws.

Finally, the definition of "consumer" is broader than the typical definition. MHMD defines the term to include not only Washington residents but also "a natural person whose consumer health data is collected in Washington." MHMD defines "collect" broadly to include activities such as accessing, retaining, acquiring, or receiving consumer health data in any manner.

MHMD excludes from the definition of consumer "an individual acting in an employment context" and states that "consumer" means a natural person who acts "only in an individual or household context."

3. Broad Definition of Consumer Health Data
MHMD applies to "consumer health data." That said, anyone trying to understand the scope of MHMD must understand that the definition of consumer health data is much broader than traditional concepts of health data.

As a starting point, MHMD defines consumer health data to include biometric information. In turn, biometric information is broadly defined as "data that is generated from the measurement or technological processing of an individual's physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data. Biometric data includes, but is not limited to: (a) Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted; or (b) Keystroke patterns or rhythms and gait patterns or rhythms that contain identifying information." Therefore, for example, face scans and voice recordings from which an identifier template ***can*** be extracted (not ***are*** extracted) are covered by MHMD even though a covered business (and consumer) may not think of them as health data.

More generally, the definition of "consumer health data" broadly states it means "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status." MHMD then lists 13 non-exclusive examples. One of those examples is "data that identifies a consumer seeking health care services." "Health care services" is broadly defined to mean "any service provided to a person to assess, measure, improve or learn about a person's mental or physical health."

During the legislative process business advocates argued that the definition could cover someone buying ginger at a grocery store because ginger can be used as a home remedy for nausea. Business advocates also argued that the definition could extend to the purchase and use of ordinary products such as groceries, athletic equipment, footwear, perfumes, jewelry, toys, and cleaning products (to name a few). An amendment to exclude these products was defeated in the Senate with bill proponents maintaining that the definition is not as broad as feared. Ultimately, the scope of this definition will likely be up to the courts to determine given the inclusion of a private right of action.

In addition, the definition of "personal information" states that it "includes, but is not limited to, data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier." This definition becomes important because, as discussed below, MHMD requires consent for the collection and sharing of consumer health data and "valid authorization" for the sale of consumer health data. Therefore, covered businesses will need to carefully think through their collection of persistent unique identifiers from Washington residents and what obligations that might trigger.

Finally, it is worth noting that there are exceptions for publicly available information, deidentified data, and information used for certain types of research.

4. Strong Consent-Based Requirements and Privacy Rights

In our prior blog post we examined MHMD's requirements in greater detail, but here is a summary of some of its more notable requirements:

Consent to Collect or Share

Regulated entities must obtain consent (a defined term) to collect or share (another defined term) consumer health data unless the collection or sharing is necessary to provide a product or service that the consumer has requested. Consent must be obtained prior to the collection or sharing and the request for consent must contain certain specified information.

Valid Authorization to Sell Consumer Health Data

Regulated entities must obtain a consumer's valid authorization to sell consumer health data. This must be done by providing the consumer with specific disclosures.

Rights

Consumers have the right to:

- Confirm whether the regulated entity is collecting, sharing or selling their consumer health data;
- Access the consumer health data;
- Obtain a list of all third parties and affiliates with whom the regulated entity has shared or sold the consumer health data and an active email address or other online mechanism to contact these third parties;
- Withdraw consent; and

- Delete their consumer health data

Privacy Policy
Regulated entities must maintain a "consumer health data privacy policy" that contains certain types of disclosures.

Geofencing
"Persons" (a term that is defined broader than regulated entities) are prohibited from implementing a geofence around an entity that provides in-person health care services under certain circumstances. This provision of MHMD does not have a delayed effective date like the data privacy provisions.

5. Quick Effective Date
For regulated entities, MHMD's data privacy provisions will go into effect on March 31, 2024. For small businesses, those provisions go into effect June 30, 2024.
CLICK HERE.

Delaware Legalizes Recreational Marijuana

Delaware became the latest state to legalize recreational marijuana on April 23, 2023 when the state's Governor failed to veto two bills that allow for the legalization of marijuana, effective immediately. Individuals who are 21 years of age and older may possess and use up to one ounce of marijuana. It will be taxed in a manner similar to alcohol.

The law provides that nothing in the law is "intended to impact or impose any requirement or restriction on employers with respect to terms and conditions of employment including but not limited to accommodation, policies or discipline." This means that employers in Delaware do not have to permit marijuana use at work or during work time and still may drug test for marijuana and take disciplinary action for positive test results.

Employers should bear in mind, however, that the use of medical marijuana still is protected under Delaware law, as it has been since 2011. The new recreational marijuana law does not change the rights of users of medical marijuana. Specifically, the Delaware Medical Marijuana Act provides, in pertinent part, that "an employer may not discriminate against a person in hiring, termination, or any term or condition of employment . . . if the discrimination is based upon either of the following: a. [t]he person's status as a cardholder; or b. [a] registered qualifying patient's positive drug test for marijuana . . . unless the patient used, possessed or was impaired by marijuana on the premises of the place of employment or during his hours of employment."

Delaware joins a growing list of states that have adult-use recreational marijuana laws. Employers should review their drug and alcohol policies frequently to ensure that they are complying with all applicable state and local marijuana laws.
CLICK HERE.

COURT CASES

No FCRA Violations Found Where Defendants Promptly Corrected Inaccurate Data and Updated Plaintiffs' Consumer Report

In a recent decision, the U.S. District Court for the Eastern District of Pennsylvania granted summary judgment in a Fair Credit Reporting Act (FCRA) case where a bank promptly corrected inaccurate mortgage payment information furnished to three national consumer reporting agencies (CRAs).

In their complaint, the plaintiffs asserted FCRA claims against the bank holding their mortgage and the CRAs alleging the bank incorrectly reported payments in forbearance were, in fact, delinquent. One plaintiff filed a dispute with one of the CRAs on August 7, 2020, which then sent notice of the dispute to the bank. The bank investigated, determined the account was reported delinquent in error, and modified its reporting to eliminate the past due amount, delete the delinquency notation, show the loan to be current, and report the loan as "paying as agreed." Two of the CRAs confirmed receiving this update and corrected the inaccuracy by September 3, 2020. The third CRA never reported the inaccurate information, so there was nothing to correct.

The plaintiffs then filed suit, alleging the bank violated § 1681s-2(b)(1) of the FCRA by failing to conduct a reasonable investigation and correct the inaccurate information after receiving a dispute from the CRA. They further alleged that the CRAs violated § 1681e(b) by not having reasonable procedures to ensure maximum possible accuracy of any information submitted and § 1681i by failing to reasonably reinvestigate the inaccurate information and properly or timely modify the inaccuracies. All defendants filed motions for summary judgment, which were granted.

Looking at the claim against the bank, the court noted a furnisher cannot be sued under § 1681s-2(b) with a claim predicated solely on inaccuracy and, instead, the plaintiff has the burden of showing the furnisher failed to conduct a reasonable investigation of the dispute. Although this is usually a question of fact, here there was no dispute the bank received the dispute on August 12, 2020, and by September 2, 2020, determined there was an error and sent the corrected information to the CRAs. Thus, it was "beyond question" the bank had complied with the requirements of § 1681s-2(b)(1) by conducting a reasonable investigation and timely providing updated information.

Moving to the claims against the CRAs, the CRAs provided detailed information about their practices, procedures, and protocols to ensure accurate and reliable data. The plaintiffs did not proffer sufficient evidence to rebut the CRAs' assertion and the court found there was no genuine issue of fact regarding the reasonableness of their procedures to ensure accuracy under § 1681e(b).

The court followed Third Circuit precedent holding § 1681i requires any CRA to reinvestigate within a reasonable time and promptly delete inaccurate or unverifiable information. The court again found that while the reasonableness of a reinvestigation is usually a jury question, here there were no genuine issues for a jury to consider. The two CRAs that reported the inaccurate information updated the plaintiffs' consumer reports after receiving notification through the ACDV process, which the court found to be an adequate and reasonable method of reinvestigation. The third CRA, which never reported the inaccurate information, could not have violated § 1681i.

Furnishers and CRAs can take comfort that despite the plaintiffs' efforts to have the bank and CRAs pay damages for a mistake that was promptly corrected, the court granted summary judgment to all of the defendants.
CLICK HERE.

Good News for Illinois Employers: Illinois Supreme Court holds that Federal Labor Law Preempts BIPA Claims

Illinois Biometric Information Privacy Act (BIPA) case law continues to develop on as the Illinois Supreme Court has issued yet another BIPA decision. This time, however, the court has provided Illinois employers with a bit of good news. In March 2023, the Illinois Supreme Court held that Illinois BIPA allegations by union-represented employees are preempted by federal law.

In *Walton v. Roosevelt Univ.*, plaintiffs alleged that as a condition of employment, Roosevelt required Walton, and other employees, to enroll scans of their hand geometry onto a biometric timekeeping device for timekeeping purposes. *Walton*

v. Roosevelt Univ., 2023 IL 128338. As the proceedings developed, Roosevelt University argued that Walton's claims under the Privacy Act were preempted by the Labor Management Relations Act (LMRA) because time keeping measures were subject to the broad management-rights clause in the CBA. Through various appeals, the Illinois Supreme Court was tasked to determine whether the LMRA preempted claims under BIPA.

In answering this question, the Court was persuaded by the federal courts' interpretations of federal law. *Walton v. Roosevelt Univ.*, 2023 IL 128338 (Mar. 23, 2023). In particular, the Seventh Circuit's decision in *Miller v. Sw. Airlines Co.* explained that under BIPA an authorized agent may receive the requisite notices and consent to the collection of biometric information. Moreover, the court found that unions were authorized agents of employees under the statute, and that the timecard management is a mandatory subject of bargaining. And, whether the union authorized use of employees' biometric data or consent to the collection of the data through a management-rights clause is a question for an adjustment board. Therefore, the Seventh Circuit held the plaintiffs' claims under BIPA were preempted by the Railway Labor Act.

Similarly, in *Fernandez v. Kerry, Inc.*, the Seventh Circuit found the preemption analysis in *Miller* applicable to section 301 of the LMRA. Id. at 646. The *Fernandez* court determined that a broad management-rights clause exists in a CBA can preempt a BIPA claim, pursuant to the LMRA, because the express language in the CBA provision stated that timekeeping and identification systems were bargaining topics between the union and management. Preemption can also occur when the CBA expressly consents to the collection of biometric data.

Applying the holdings of *Miller* and *Fernandez* the Illinois Supreme Court found that when an employer invokes a broad management rights clause from a CBA, such clause will preempt a BIPA claim brought by bargaining unit employees. Thus, the court held that Walton's Privacy Act claims are preempted by the LMRA.

This decision is in favor of employers who employ union-represented employees and suggests that employers review their CBAs and management rights provisions. This ruling, similar to the ruling in *Tims*, highlights the precautionary measures employers should implement to ensure compliance with BIPA.
CLICK HERE.

INTERNATIONAL DEVELOPMENTS

European Data Protection Board Opinion on the Draft Adequacy Decision for the EU-US Data Privacy Framework

On February 28, 2023, the European Data Protection Board (the "**EDPB**") published its opinion (the "**EDPB Opinion**") on the European Commission Draft Implementing Decision (the "**Draft Decision**") on the adequate protection of personal data under the **EU-US Data Privacy Framework**, based on the new privacy rules introduced in the United States with Executive Order 14086.

The Draft Decision
The Draft Decision (available here) was published by the European Commission on December 13, 2022, pursuant to Article 45 of the GDPR. In the Draft Decision, the Commission concluded that the EU-US Data Privacy Framework provided safeguards comparable to those granted under EU law, because

- any interference with individuals' fundamental rights in the public interest is limited to the strictly necessary; and
- effective legal protection against such interference is provided.

Once adopted, it will enable the transfer of data to the United States, following invalidation of the previous adequacy decision on the EU-US Privacy Shield by the Court of Justice of the European Union.

The EDPB Opinion
The EDPB Opinion constitutes the first step in the process of adopting the adequacy decision on the EU-US Data Privacy Framework.

Overall, the EDPB acknowledged substantial improvements over the Privacy Shield, but at the same time it noted some concerns and requested clarification on certain points, namely:

- **General concerns**: The EDPB called for more context regarding U.S. legislation in the Draft Decision, which is frequently referenced in the EU-US Data Privacy Framework. According to the EDPB, there is lingering uncertainty as to the effectiveness of the scope of the obligations set forth in the EU-US Data Privacy Framework. Additionally, the EDPB noted a general lack of clarity throughout the document, in part due to inconsistent terminology.

Additionally, the EDPB stressed the need to define terms and concepts that may be interpreted differently in the EU and the United States. The EDPB also mentioned critical issues regarding an individual's right of access, right of object, and right not to be subject to decisions based solely on automated processing.

There is also concern regarding dissemination of data to U.S. authorities that would enable them to obtain data that they would not have been allowed to collect directly. Similar criticism concerns onward transfers, *i.e.*, dissemination to additional recipients outside the U.S. government, including foreign governments and international organizations. Indeed, the lack of controls on onward transfers may undermine the level of protection ensured by original recipients in the United States.

- **Enforcement mechanisms**: The EDPB reiterated concerns regarding the (self) certification mechanism provided by the EU-US Data Privacy Framework. According to the EDPB, under the Privacy Shield this mechanism proved to be ineffective (as a mere formality). The EDPB therefore called for effective oversight as part of periodic reviews.
- **Redress mechanisms**: The EDPB considered the new redress mechanisms a significant improvement over the previous mechanisms under the Privacy Shield. Nevertheless, the EDPB stressed the need to assess the genuine independence of the two relevant bodies, the Privacy and Civil Liberties Oversight Board and the Data Protection Review Court, as well as the need for the European Commission to monitor the functioning of these mechanisms.
- **Access and use of personal data by U.S. public authorities**: The EDPB praised the introduction of the concepts of necessity and proportionality into the U.S. legal framework on signals intelligence, which shall now be conducted only to the extent necessary for validated intelligence priority collection and only to the extent and in a manner proportionate to that priority.

However, the EDPB noted that the requirements set forth in Executive Order 14086 need to be further implemented by U.S. agencies. Therefore, the EDPB recommended that the European Commission make the adoption of the final decision conditional upon implementation of Executive Order 14086 by U.S. agencies. The EDPB also called for clarification regarding the retention rules applicable to personal data.

The EDPB also looked at bulk collection of personal data. As this involves large quantities of data collected indiscriminately, it presents greater risk for individuals than targeted collection and thus requires additional safeguards. The EU-US Data Privacy Framework provides that data collected in bulk shall be used in pursuit of one or more of six listed objectives, but the EDPB noted that that form of collection remains largely accessible. Moreover, the EDPB demanded introduction of specific safeguards for automated decision-making and profiling, namely to ensure purpose limitation, prior independent authorization, rules on data retention, and safeguards regarding dissemination.

The EDPB also stressed the need to verify accurately the number and scope of exemptions from the duty to adhere to the principles set out in the EU-US Data Privacy Framework, which may reduce the effectiveness of its safeguards. Additionally, the EDPB called for greater clarity regarding implementation and function of the principles of proportionality, purpose limitation, and necessity (for instance, in the context of application of FISA Section 702).

- **Periodic reviews**: The EDPB suggested that the Commission carry out periodic reviews of the adequacy decision every three years.

Next steps for the draft adequacy decision
The EDPB Opinion marked the first step in the process of adopting the adequacy decision on the EU-US Data Privacy Framework. Another step has already been taken: the European Parliament Committee on Civil Liberties, Justice and Home Affairs has expressed its opinion as well. It challenged the assessment carried out in the Draft Decision, stating that the EU-US Data Privacy Framework does not ensure an adequate level of protection. The full Parliament vote on the resolution on the adequacy of protection afforded by the EU-US Data Privacy Framework is expected to take place in the coming months. We will see then how much weight the Commission gives to these non-binding opinions as part of the process of adopting the Draft Decision.
CLICK HERE.

No Action for Theft of Personal Information Without Loss

Theft of personal information does not by itself entitle the victim to damages in Canada; proof of loss or harm is required, the Alberta Court of Appeal held recently in *Setoguchi v Uber BV*. This, and other recent decisions, demonstrate that plaintiffs cannot easily win large awards in data breach class actions. This is good news for firms that suffer data breaches. But firms still need robust cybersecurity safeguards to lessen their chances of being hacked, as data breaches have other costly consequences.

Theft of Personal Information from Uber Leads to Class Action
In 2016, rideshare company Uber suffered a data breach. Hackers stole the personal information of about 57 million Uber drivers and customers. The stolen information consisted of names, phone numbers, and email addresses (as well as some U.S. driver's license numbers). Uber paid the hackers a $100,000 ransom to destroy this data.
After the breach became public, Setoguchi, an Uber customer, commenced a class action.

The Alberta Court of King's Bench refused to certify the class. It found that a class action would not be the preferable procedure to resolve the common issues because the only damages that might be common to the class would be nominal and *de minimis*.

Setoguchi appealed.

Inherent Value of Personal Information Cannot Ground a Negligence Claim
The appeal court also focused on the plaintiff's theory of loss. This was important as loss was an essential element of the plaintiff's negligence claim.

The plaintiff had pleaded that class members suffered loss, but it is not enough merely to state that loss was suffered, the court noted. Rather, "a plaintiff is required to plead facts sufficient to amount *at law* to damage."

The plaintiff argued that the action should be certified on the basis of the "first loss." This first loss arises because personal information has inherent value. Its theft thus gives rise to a loss that is common to the class. The plaintiff seems to have adopted this approach in order to get around the problem that there was no evidence of any consequential loss or harm to the class. Even if there were consequential losses, they likely could not be proven on a class-wide basis, but would instead require individual inquiries.

The appeal court rejected this first loss theory. "A claim for either nominal or symbolic damages cannot ground a claim in negligence," the court held. Though the theft of "publicly available information" might make class members "marginally 'worse off,'" this loss is negligible or trivial and not real. It does not "rise above the ordinary annoyances, anxieties, and fears that people living in society routinely accept," as the Supreme Court put it in *Mustapha v Culligan of Canada Ltd.*

As a result, the court held that the negligence claim did not disclose a cause of action.

Class Actions Not Preferable Procedure for Nominal Damages Claims

While the plaintiff's breach of contract claim did not require proof of loss, they would only be entitled to nominal damages in a "trivial" amount. Because of this, a class action would not be the preferable procedure for resolving the breach of contract claims. It would not improve access to justice to certify a case that seems "hopeless for recovery of actual losses."

Judicial Skepticism in Data Breach Cases?

The *Uber* case is remarkably similar to the 2021 decision of the Quebec Superior Court in a proposed class action against the Investment Industry Regulatory Organization of Canada (IIROC). An IIROC employee had left an unencrypted laptop containing sensitive information of about 50,000 investors on a train. There was no evidence of any actual misuse of this data. In two separate class actions, one started by Sofio, and the other, by Lamoureux, the Quebec court held that stress suffered by class members did not amount to compensable injury; as in *Uber*, it did not rise "above the ordinary annoyances, anxieties, and fears that people living in society routinely, if sometimes reluctantly, accept." The Quebec Court of Appeal dismissed appeals in both cases.

Uber also follows on the heels of the Ontario Court of Appeal's refusal, in late 2022, to extend liability for the tort of intrusion upon seclusion to defendants that have been hacked by third parties. That case, *Owsianik v. Equifax Canada Co.*, arose as a result of a 2017 hack of personal information stored by Equifax, a credit reporting service. The plaintiffs contended that Equifax was liable for the tort of intrusion upon seclusion because it failed to take appropriate steps to safeguard sensitive financial information it stored.

The tort of intrusion upon seclusion is an intentional tort, however. One of its essential elements is that the *defendant* must have unlawfully invaded or intruded upon the plaintiff's private affairs or concerns. It was the hackers, not Equifax, that had invaded the plaintiff's privacy. "There is simply no conduct capable of amounting to an intrusion into, or an invasion of, the plaintiff's privacy alleged against Equifax in the claim." Negligent storage of information cannot amount to an intrusion, the court held.

While these cases suggest judicial skepticism about class actions seeking compensation from firms that are hacked, not all defendants have met with equal success. For example, in *Tucci v. Peoples Trust Company*, the British Columbia Court of Appeal largely upheld a decision to certify a data breach class action arising out of a data breach suffered by Peoples Trust. In that case, the court of appeal seems to have accepted that nominal damages could be "awarded to acknowledge the commission of a legal wrong where no actual loss is proven."

Robust Cybersecurity Safeguards Still Needed

Apart from class action liability, data breaches can trigger large fines and important reputational consequences.

In Canada, as in many other jurisdictions, data breaches that pose a real risk of harm to individuals must be reported to the Office of the Privacy Commissioner. Canada's proposed new Consumer Privacy Protection Act, which is currently before Parliament as Bill C-27, provides for administrative monetary penalties (AMPs) of up to $10 million, or 3% of an organization's gross global revenue, for failures to adequately safeguard personal information. A statutory cause of action will also enable consumers to recover loss or injury caused by breaches of the new law.

Data breaches can potentially also give rise to penalties under Canada's *Competition Act* if, for example, the breach shows that claims made by a firm about its privacy protections were false or misleading.

In an era when it is commonplace for firms to be the victim of data breaches and ransomware attacks, firms must maintain robust safeguards against cyberattacks and have an emergency plan for dealing with the fallout from a successful cyberattack.
CLICK HERE.

Failure to Provide Information about Personal Data in Germany Can be Costly

If an employee of a company wishes to obtain information about their processed personal data and the company fails to comply, this can potentially be costly. In this context, the German Federal Labour Court [Bundesarbeitsgericht, BAG] was also against an obligation to represent and prove the concrete occurrence of damage in the event of a failure to provide information. A final decision by the ECJ is pending, however. We explain what companies need to watch out for in this connection.

Current case law on the claim to information and damages under the GDPR
With the entry into force of the GDPR 2018, companies were faced with numerous questions concerning the protection of their employees' personal data. Since then, not only does all processing of employees' personal data require approval pursuant to Art. 6 (1) GDPR, but employees are also entitled to request information about the data processed by their employer.

The claim to information pursuant to Art. 15 GDPR includes not only the employee's right to know *whether* data is being processed, but also *which* data this involves. Employees can also request from their employer a copy of such personal data (Art. 15 (2) sentence 1 GDPR). In this case, the employing company must provide the information no later than one month after the request (Art. 12 (3) sentence 1 GDPR). If the information is not provided or not provided in a timely manner, the employee has a claim to non-material damages pursuant to Art. 82 (1) GDPR.

In the recent past, the labour courts have increasingly dealt with the questions of whether and to what extent an employer is obligated to provide information, and whether and under what conditions a damage claim exists if such information is not provided.

For example, the Regional Labour Court [*Landesarbeitsgericht, LAG*] of Hamm ruled on 02 December 2022 (docket No.: 19 Sa 756/22) that a judicial request for information that merely repeats the wording of Art. 15 (1) of the GDPR is inadmissible on grounds of lack of specificity if the employing company has already partially fulfilled the employee's request for information. In this case, namely - according to the LAG Hamm - it would be possible for the employee to specify the request for information.

However, it deemed a possible non-material damage claim pursuant to Art. 82 (1) GDPR to be independent of this. In this context, the Austrian Supreme Court had already referred the question to the European Court of Justice (ECJ) for a preliminary ruling on 15 April 2021. It was to determine whether, besides a violation of provisions of the GDPR, a further prerequisite for awarding damages was that the data subject has suffered damage, or whether the violation of provisions of the GDPR as such sufficed to acknowledge the claim (docket No: C-300/21). The ECJ's decision is still pending.

In the same year, the BAG also referred a question to the ECJ in this connection, namely whether the plaintiff bears the burden of representation and proof of the existence of non-material damages (BAG, decision dated 26 August 2021 - 8 AZR 253/20). Here as well, we await the response from Strasbourg (docket No. C-667/21).

However, pending the ECJ's decision, the provisional legal opinion of the BAG is that the violation of the GDPR in itself leads to non-material damages to be compensated and that the existence of actual damage is not relevant (BAG, judgement dated 05 May 2022 - 2 AZR 363/21).

Following the provisional opinion of the BAG, the Labour Court [*Arbeitsgericht, ArbG*] of Oldenburg recently awarded a plaintiff employee a claim to compensation for their non-material damages in an amount of 500 euros per month (ArbG Oldenburg, judgement dated 09 February 2023 - 3 Ca 150/21). The total damage to be compensated by the employing

company was 10,000 euros. The court deemed it unnecessary for the employee to represent and prove the existence of (non-material) damage; the violation of the GDPR itself sufficed. The ArbG Oldenburg also followed the line taken by the BAG with regard to the amount in dispute, namely that the order to pay damages for failing to provide information should have both a preventive and deterrent character.

This legal opinion was not shared by the LAG Hamm, however, which rejected the damage claim of the plaintiff employee in its decision of 02 December 2022 (docket No. 19 Sa 756/22) on grounds that she had not fulfilled her burden of representation and proof of the occurrence of damage. The LAG Hamm justifies its legal opinion by stating that Art. 82 of the GDPR does not constitute a "compensation of punitive damages" that is independent of the existence of a concrete damage. Due to the deviation from supreme court case law, however, the LAG allowed an appeal to the BAG.

Conclusion
At present, based on the provisional case law of the BAG, we can assume that employees who request information from their employer do not have to prove concrete non-material damage in order to assert a damage claim under Art. 82 (1) of the GDPR. Even though there are individual decisions - such as that of the LAG Hamm – that do not support the BAG's provisional view, we must ultimately await a final decision of the ECJ before gaining legal certainty. In order to avoid damage claims by employees, companies are therefore still well advised to comply with requests for information by employees within the meaning of Art. 15 (1) of the GDPR.

In this case, however, if the employing company has already (partially) fulfilled the request for information, employees then have an increased obligation in labour court proceedings to provide more specific information when filing their complaint. Accordingly, companies should comply with the request for information to the greatest extent possible in order to increase the procedural requirements. Otherwise, the mere repetition of the wording of Art. 15(1) GDPR is sufficient in the context of the complaint.
CLICK HERE.

At a glance: data protection and management of health data in France

Definition of 'health data'

What constitutes 'health data'? Is there a definition of 'anonymised' health data?
Health data is defined at an EU level. The General Data Protection Regulation (GDPR) provides in article 4.15 that health data is personal data 'related to the physical or mental health of the natural person, including the provision of healthcare services, which reveal information about his or her health status'.

Given the terms of article 9 of the GDPR, health data, alongside genetic and biometric data, are considered particularly sensitive personal data.

Additionally, the French Commission for Data Protection and Liberties (CNIL) has a broad interpretation of the notion and considers three categories of data that are to be considered as health data:

- health data by nature (data from medical history, illness, care services, test results, treatments, etc);
- health data because of their medical purpose (sexual orientation, etc); and
- data that becomes health data due to the cross-referencing of other data that allows for the health state or health risks of a person to be determined (cross-referencing of blood pressure with measurement of efforts or the number of steps, etc).

Anonymised health data refers to anonymised personal data and is excluded from the scope of the GDPR. The preamble of the GDPR defines, in the negative, anonymised personal data as 'information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'.

At a French level, the CNIL provides, with a definition of anonymised health data, 'a form of data processing that consists in using a set of techniques in such a way as to make impossible, in practice, any identification of the person whose personal data is being processed, irreversibly'.

Anonymised health data should not be confused with pseudonymised data that results from the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (see article 4.5 of the GDPR).

As for now, three criteria have been elaborated at an EU level, and followed in France, to verify the robustness of each anonymisation technique, namely:

- is it still possible to single out an individual;
- is it still possible to link records relating to an individual; and
- can information be inferred concerning an individual?

Data protection law

What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

In France, health data were initially protected by Law No. 78-17 of 6 January 1978 regarding information technology and data protection. Law No. 2018-493 of 20 June 2018 on personal data protection amended adapts French legislation to comply with the GDPR.

These regulations classify health data as sensitive data, such as genetic data or biometric data. Data processing is therefore subject to additional alternative conditions, such as:

- the individual has given their explicit consent;
- the processing is necessary for the purposes of preventive or occupational medicine;
- medical diagnosis;
- the provision of health or social care treatment; and
- for reasons of public interest in the area of public health.

At a national level, health data is considered specifically sensitive and the CNIL has developed specific guidance about health data processing to facilitate health data processing.

Nevertheless, the processing of health data may be subject to a prior CNIL authorisation if the process of health data does not comply with reference standards set up by the CNIL. The CNIL will assess the purpose of the data processing, the data concerned, measures taken to ensure the safety of data processing, etc.

Anonymised health data

Is anonymised health data subject to specific regulations or guidelines?

Regulations on personal data no longer apply as the dissemination or reuse of anonymised data has no impact on the privacy of the person concerned. Therefore, anonymised health data fall outside the scope of personal data regulations (conversely, the process of anonymisation is still a process of personal data that is subject to personal data regulations).

Nevertheless, it is still necessary to take into account Regulation (EU) 2018/1807 of 14 November 2018, establishing a framework for the free flow of non-personal data in the European Union and following parliamentary discussion over the proposition for a data act, launched by the European Commission on February 2022 regarding personal and non-personal data, which aims to propose new rules on the use and access to data generated in the EU across all economic sectors, including the health sector.

Enforcement

How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

The CNIL applies and enforces the regulations on personal data by imposing administrative sanctions, which can range from a reminder of the applicable regulation to an administrative fine.

Infringement of these regulations can also constitute a criminal offence, which can be referred to criminal courts.

Several financial penalties have already been implemented against different companies and healthcare professionals, the highest financial penalty being against Google LLC and Google Ireland Limited of €60 million and €40 million respectively. On November 2022, the CNIL made a statement in response to numerous complaints against private supplementary insurance organisations that use health data generated by healthcare professionals to reimburse insured patients. The CNIL decided not to sanction those organisations but considers the regulatory framework regarding these organisations insufficient regarding data protection and medical secrecy.

Cybersecurity
What cybersecurity laws and best practices are relevant for digital health offerings?

In terms of cybersecurity, Directive (EU) 2016/1148 of 6 July 2016 (NIS Directive) transposed in France by Decree No. 2018-384 of 23 May 2018, affects digital health companies as digital services providers. Public and private health infrastructures are considered necessary service providers and are subject to strengthened measures to manage risk to the security of their network and information systems.

This Directive defines an EU certification framework and a notification process for the management of incidents impacting the IT system that significantly affects the continuity of the services they provide, to the dedicated cybersecurity authority. A second NIS Directive was enacted on December 2022 (Directive (EU) 2022/2555), which may be transposed in France within two years.

Best practices and practical tips
What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

Before the launch of a digital health solution, it is necessary to determine:

- the type of data that is to be processed: if it is health personal data, it is important to check if anonymisation is possible, or whether only pseudonymisation remains possible for the data processing of the solution. If anonymised data is required for the digital solution, the entity may seek data already pseudonymised by a third party, rather than processing data to obtain anonymised data;
- the entity that hosts the data, as a health data host needs a ministerial authorisation for data storage, according to article L1111-8 of the FPHC. Companies are also encouraged to select existing data hosts. All agreements with subcontractors regarding these data must be drafted unambiguously, with exhaustive documentation of the subcontractor's activity and guarantee in terms of cybersecurity and compliance with personal data regulations where appropriate; and
- the information communicated to data subjects regarding the process and reuse of health data, where appropriate. The company must be the most transparent possible and take measures to obtain explicit consent from him or her.

CLICK HERE.

Kingdom of Saudi Arabia Approves Amendment to Personal Data Protection Law

On March 27, 2023, the Kingdom of Saudi Arabia (KSA) Council of Ministers approved a series of 27 amendments (the Amendments) to the KSA Personal Data Protection Law (PDPL) pursuant to Royal Decree No. M148 of 05/09/1444H (the text of the Amendments is available in Arabic only here and the text of the consolidated PDPL reflecting the Amendments is available in Arabic only here). The PDPL constitutes the country's first comprehensive national data protection legislation and was initially published on September 24, 2021, pursuant to Royal Decree M/19 of 9/2/1443H. Since its initial publication, there have been a series of developments, including the Saudi Data and Artificial Intelligence Authority (SDAIA) announcing that full enforcement of the law had been postponed, the issuance of draft executive regulations supplementing the PDPL and a public consultation on proposed amendments to the PDPL by the SDAIA in November 2022 (as to which see our previous blog post here). The Amendments reflect some, but not all, of the amendments proposed in the public consultation, as further discussed below.

The PDPL regulates the processing of personal data relating to an individual in the KSA by any means, including where such processing is conducted by a party outside the KSA, and further establishes certain novel rights for individuals in relation to how their personal data is processed by data controllers (with consent being at the forefront), and creates new obligations for data controllers to adhere to. Following the approval of the Amendments, organizations operating in the KSA should promptly begin taking practical steps to ensure compliance. While compliance with existing international data protection laws, such as the European Union's General Data Protection Regulation (GDPR), may be beneficial, the unique features of the PDPL must be taken into consideration.

The Amendments implement significant amendments to the previous version of the PDPL, notably including:

- **Amendment of Definitions**: The Amendments amend a number of definitions in Article 1 of the PDPL, including narrowing the definition of "Sensitive Personal Data" by removing the prior references to membership in a civil association or institution, credit data and location data (and instead now referring solely to personal data relating to an individual's ethnic or racial origin, religious, intellectual or political belief, criminal and security data, biometrics data, genetic data, health data and data indicating that one or both parents of an individual is unknown), and amending the definition of "Owner of Personal Data" to remove the previous extension to an individual's legal representative or guardian (such that it now refers only to the individual to whom the personal data relates).
- **Written Consent vs. Explicit Consent**: The Amendments no longer require consent to be in writing, instead requiring consent to be "explicit."
- **Legitimate Interests Lawful Basis**: One of the most significant amendments approved by the Amendments is the inclusion of legitimate interests as a lawful basis for processing data, although the term is not further defined under the PDPL. Pursuant to the Amendments, (1) the processing of personal data under the PDPL is not subject to the requirement for consent in Article 5 of the PDPL where the processing is necessary to achieve the legitimate interests of the controller, and (2) a controller may collect personal data directly from a person other than the owner or may process such data for purposes other than the purpose for which it was collected where such collection or processing is necessary to achieve the legitimate interests of the controller, in each case unless such processing prejudices the rights of the owner of the personal data or conflicts with their interests and provided such data is not sensitive personal data. Furthermore, whereas a data controller could previously only disclose personal data in five prescribed circumstances, the Amendments now also permit disclosure if it is necessary to achieve the legitimate interests of the controller, provided such disclosure does not prejudice the rights of the owner of the data, conflict with their interests or constitute sensitive personal data.
- **International Data Transfers**: Another significant amendment approved under the Amendments is the extension of the data transfer provisions. Previously, data controllers were prohibited from transferring personal data outside of the KSA (except in cases of extreme necessity to preserve the life of the data subject outside of the KSA or their vital interests, or to prevent, examine or treat a disease), unless such transfer was in the implementation of an obligation under an agreement to which the KSA was a party or to serve the interests of the KSA and only after four prescribed conditions were met, including the approval of the competent authority for the transfer or disclosure. Pursuant to the Amendments, a data controller may transfer personal data outside of KSA in order to achieve certain prescribed purposes (retaining the two previous grounds under the initial draft of the PDPL, namely to serve the interests of the KSA or in the implementation of an obligation under an agreement to which the KSA is a party, and the exception for cases of extreme necessity, the vital interests of the data subject and relating to disease), notably now including if it is in implementation of an obligation to which the owner of the personal data is a party and if it is in implementation of other purposes specified in the regulations (which were previously not grounds on which a data transfer was permissible). The conditions that must be met when transferring or disclosing personal data outside of the KSA are further confirmed (retaining the previous requirement that the transfer should be limited to the minimum amount of personal data required and that the transfer shall not prejudice the national security or vital interests of the KSA), although the requirement to seek the approval of the competent authority in respect of the transfer or disclosure has now been removed and the Amendments now include the requirement that there shall be an appropriate level of protection for the personal data outside of the KSA (which must not be less than the level of protection stipulated in the PDPL and the associated regulations—previously the PDPL required that sufficient guarantees be provided to preserve the personal data being transferred and for the confidentiality of such data to be preserved at a standard not less than that stipulated

by the PDPL or the regulations). The executive regulations supplementing the PDPL shall specify the provisions, standards and procedures relating to the application of the data transfer provisions, including determining the circumstances in which a controller may be exempt from compliance with any of the prescribed conditions.

- **Repeal of Electronic Register Requirement**: The Amendments repeal Article 32 of the PDPL, which previously provided that the competent authority shall establish an electronic portal for the purposes of building a national register of controllers and requiring all data controllers to register in the portal.
- **Data Breach Notification**: Previously, if the leakage of, damage or unauthorized access to personal data would cause serious harm to the personal data or the owner of the personal data, the controller was required to notify such person "immediately." This timing requirement has been removed under the Amendments; instead, a controller must notify the owner of personal data of any leak, damage or unauthorized access to personal data that may result in damage to such data or conflict with the person's rights or interests, as shall be further specified in the regulations.
- **Penalties for Non-Compliance**: Previously, any person found to violate the data transfer provisions of Article 29 of the PDPL was subject to punishment by imprisonment for a period not exceeding one year and/or a fine not exceeding 1,000,000 Saudi Riyals. The Amendments no longer include this penalty, but retain the penalty of imprisonment for a period of two years and/or a fine not exceeding 3,000,000 Saudi Riyals where a person discloses or publishes sensitive personal data in violation of the PDPL (where such disclosure or publication is made with the intention of harming the owner of the data or achieving a personal benefit). Administrative fines of up to 5,000,000 Saudi Riyals may also be issued for any other violation of PDPL.
- **New Effective Date**: Pursuant to the Amendments, the PDPL shall now enter into force 720 days after the publication of the original law in the KSA Official Gazette such that the PDPL shall be effective from September 14, 2023. However, data controllers have a one-year grace period in order to comply with the PDPL (i.e., September 14, 2014). Executive regulations supplementing the PDPL are due to be issued in advance of this effective date and will likely provide further detail and clarification as to the provisions of the PDPL.

As the effective date approaches, businesses that are required to comply with the new PDPL should start examining their data processing activities, including any cross-border data transfers, to ensure timely compliance with the PDPL. To achieve this, businesses may want to:

1. Create or update existing policies and procedures related to data protection.
2. Provide training for employees on the key provisions and significance of the PDPL.
3. Appoint a data protection officer to oversee compliance efforts (noting that the PDPL expressly states that the executive regulations shall specify the circumstances in which a controller must appoint or designate a person as a personal data protection officer).
4. Conduct regular audits and assessments of data protection practices.
5. Implement privacy-by-design and privacy-by-default principles in new projects and systems.
6. Establish a process for handling data subject requests, such as data access, rectification, or deletion.
7. Develop a clear procedure for reporting data breaches to the appropriate authorities.
8. Regularly update and review data protection measures to maintain compliance with the evolving legal landscape.

CLICK HERE.

MISCELLEANOUS DEVELOPMENTS

Multiple States Considering Legislation to Ban Weight Discrimination in Employment

he Americans with Disabilities Act (ADA) prohibits discrimination in employment on the basis of disability, including "morbid obesity." However, outside of this condition, the ADA's protections do not extend to employees who allege that they have been discriminated against based on their weight. In recent years, activists opposed to such discrimination have pushed for the adoption of new laws to add weight to the list of protected categories under state and local employment discrimination laws.

Currently, several states and municipalities are considering such proposals. These include measures introduced in Massachusetts, New Jersey, New York State, and New York City. These laws would ban discrimination on the basis of weight in hiring, employee benefits, and other terms and conditions of employment. Some of these proposals include exceptions if the employer can demonstrate that a weight restriction is necessary to safely and effectively perform the job.

These types of legislative efforts tend to come in waves, meaning that adoption by one state encourages similar measures in others. Even without a specific law in their jurisdictions, employers may want to consider including weight and appearance in general in their employee anti-discrimination training.
CLICK HERE.

Enforcement Deferral Available for California Pay Data Reports on Labor Contractor Employees

In 2022, the California legislature passed Senate Bill (SB) 1162, which expanded the state's existing pay data reporting requirements for "payroll employees" to include a new pay data report for employers with 100 or more "labor contractor employees." Under SB 1162, the pay data reporting deadline was moved to May. This year these reports are due May 10th.

But—according to a new FAQ from the California Civil Rights Department—beginning April 18, employers may seek "enforcement deferral" on their "labor contractor employee reports." This delayed enforcement may come as a pleasant surprise to employers still grappling with the expanded scope of the labor contractor reporting.

The key takeaways from the April 14th FAQ Update include:

- The CRD will only accept requests for enforcement deferral through its pay data reporting portal. As such, employers interested in taking advantage of this reprieve must first register for the portal.
- Request for enforcement deferral must be made by May 10, 2023.
- The enforcement deferral will be through July 10, 2023.
- The CRD will not consider requests made by a third party on behalf of an employer, such as a Professional Employer Organization (PEO).
- The enforcement deferral request will only apply to "labor contractor employees" reports. Reports covering "payroll employees" will still be due on May 10th.

Under applicable pay data reporting requirements, the CRD may seek a court order requiring the employer to comply with reporting requirements if they do not submit timely, as well as civil penalties of up to $100 per employee for initial violations. Employers with concerns over the May 10th "labor contractor employee" reporting deadline may benefit from seeking taking advantage of this procedure to seek enforcement deferral.
CLICK HERE.

New York Releases New Changes to its Model Sexual Harassment Policy and Training Video

On April 11, 2023, the New York State Department of Labor released updated versions of its sexual harassment model policy and training materials.

New York employers have been required since 2018 to adopt a written sexual harassment policy that meets certain minimum standards, and to implement annual anti-harassment training for employees. New York employers must also provide employees at the time of hiring and annually during training with a copy of the policy. To help employers comply, the New

York Department of Labor issued model forms, including a model policy, and a model training video. The changes to the model policy and training video are significant. Here's what all New York employers need to know:

- In explaining that sexual harassment is a form of "gender-based" discrimination, the new policy now provides a detailed explanation of gender diversity including definitions of cisgender, transgender and non-binary persons.
- In describing the legal standard in New York, the new policy adds that sexual harassment does not need to be severe or pervasive to be illegal; that intent is irrelevant under the law; and that whether conduct is harassing will be considered from the perspective of a "reasonable victim of discrimination with the same protected characteristics."
- The new policy provides an updated, non-exhaustive list of examples of sexual harassment and retaliation, including repeated requests for dates and gift giving, asking employees to take on traditionally gendered roles, or having different expectations of employees with children.
- The new policy makes clear that harassing behavior can happen in the remote workplace, such as in virtual meetings or after hours on personal cell phones.
- The new policy includes a provision in the section on "Supervisory Responsibilities" and the section on "Complaints and Investigations" telling supervisors and managers to be mindful of the impact investigations into sexual harassment can have on victims, and to handle such matters with sensitivity.
- The new policy adds a brand new section on bystander intervention, which explains the "five standard methods of intervention" that can be used if employees witness harassment or discrimination.
- The new policy includes the state's confidential hotline for complaints of workplace sexual harassment in the section on "Legal Protections and External Remedies".
- The new policy adds a "Conclusion" section stating that while the focus of the policy is on sexual harassment and gender discrimination, the New York State Human Rights Law protects against discrimination in other protected classes including sex, sexual orientation, gender identity or expression, age, race, creed, color, national origin, military status, disability, pre-disposing genetic characteristics, familial status, marital status, criminal history, or domestic violence survivor status, and that the policy "should be considered applicable to all protected classes."
- The New York Department of Labor has also released a new training video, which can be found here. The video meets all New York State training requirements except for being interactive; however, the New York Department of Labor provides employers with a method for meeting this requirement.

Employers should carefully review the latest materials and update their policies and training materials. As a best practice, employers should also customize policies and training to their specific organization.
CLICK HERE.

New York Releases Data Security Guide to Help Businesses Protect Personal Information

On April 19th, New York's Attorney General, Letitia James, released a document titled, "*Protecting consumer's personal information: Tips for businesses to keep data safe and secure"* (the "guide"), a resource to help businesses adopt effective data security measures. It draws on the Office of the Attorney General's ("OAG") experience investigating and prosecuting cybersecurity breaches, and highlights findings from such investigations. The guide can be found here.

Just last year, OAG investigated multiple large companies for inadequate cybersecurity practices. OAG obtained a USD$1.25 million settlement with Carnival Cruise Line following the unauthorized access of employee email accounts which exposed customers' sensitive personal information, settled with T-Mobile after its failure to provide sufficient vendor oversight leading to the unauthorized access of customer information stored on a vendor's network, and reached a USD$400,000 settlement with Wegmans after the supermarket chain's cloud storage containers were inadvertently configured to allow public access. Overall, 4,000 data breach incident notifications were received by the OAG in 2022, providing ample opportunity for OAG to exercise its enforcement discretion.

The guide recommends data practices that companies should adopt to protect their systems. The recommendations from the guide include:

1. **Maintain controls for secure authentication**, with a preference for multi-factor authentication and strong password requirements.
2. **Encrypt sensitive customer information**.
3. **Ensure service providers use reasonable security measures**, including carefully selecting service providers, building security expectations into contracts, and monitoring service providers.
4. **Know where you keep consumer information** to prevent unauthorized and public access.
5. **Guard against data leakage in web applications**, including by masking sensitive information.

6. **Protect customer accounts impacted in data security incidents,** including resetting passwords of accessed accounts and notifying impacted users when necessary.
7. **Delete or disable unnecessary accounts**, which may be vulnerable to unauthorized access.
8. **Guard against automated attacks.** Tips specific to this recommendation can be found in an earlier guide on credential stuffing attacks, here.
9. **Provide clear and accurate notice to consumers**. Misleading statements following a data breach can violate New York Law.

Although this guide does not constitute a legal requirement or official New York State policy, the OAG hopes companies implement its recommendations to lower their risk of data breaches. It is likely that these measures will become part of the suite of best practices adopted by the privacy sector to mitigate risk, including on the litigation front, where the adequacy of a company's cyber controls in the wake of a data breach continues to be an area of focus by the plaintiff's bar. Privacy World will continue to cover cybersecurity and data privacy developments in New York and beyond.
CLICK HERE.

Breach of Personal Information Notification (BPIN) Act Amendment

Important amendments to Pennsylvania's data breach law – the Breach of Personal Information Notification Act (the "Act") – will take effect May 3, 2023. This is an important update to Pennsylvania data privacy laws as the legislature attempts to provide additional data protections to the Commonwealth's citizens.

The Act requires notification to Pennsylvania residents whose personal information data was or may have been disclosed due to a breach of the security of a company's or other entity's system. Similar to other states' data breach notification statutes, the amendment (in November) expanded the definition of "personal information." This expanded definition includes medical and health information, and a user name or email address in combination with a password or security questions and answers that would permit access to an online account.

These items now included in the definition of personal information are in addition to the categories of personal information that all states regulate – such as names in conjunction with driver's license and social security numbers.
The Act defines a "breach of the security of the system" as "unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals . . .."

As it stands today, the Act requires notification when a "discovery" has been made that there was a security breach. Beginning May 3, the Act will require notification when a "determination" of a breach has been made. According to the definitions included in the Act and amendment, a "discovery" occurs when the entity has "[t]he knowledge of or reasonable suspicion" that a breach has occurred, while a "determination" occurs when the entity has "[a] verification or reasonable certainty" that a breach has occurred. This is clearly a more "entity-friendly" version of the act, as the company is able to verify a breach before performing notifications.

As an additional improvement to the process of coordinating data reach responses, entities will now be allowed to provide email notice to affected data subjects when the breach involves a user name or email address, in combination with a password or a security question and answer, that could be used to allow access to an online account. An email notice will be permitted under these circumstances if the email directs the individual to promptly change his or her information or to take other appropriate steps to protect the individuals online accounts.

In summary, the new amendment is an improvement for both companies and Pennsylvania citizens. The notification process is improved, as well as the fact that companies can now verify a breach before notification requirements set in.
CLICK HERE.