MAY 2024

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 | MAY 2024

ClearStar is happy to share screening 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.

EXECUTIVE SUMMARY

May 2024 Screening Compliance Update Executive Summary

The screening compliance landscape witnessed some major changes that have been documented in the MAY 2024 SCREENING COMPLIANCE UPDATE. Below is an EXECUTIVE SUMMARY of some of the new developments at the FEDERAL, STATE, COUNTY, and INTERNATIONAL levels.

- FEDERAL DEVELOPMENTS: The U.S. Drug Enforcement Administration (DEA) announced that it will propose to reclassify marijuana from a Schedule I drug to a Schedule III drug. The U.S. Department of Justice (DOJ) also announced that the Attorney General submitted a notice of proposed rulemaking initiating a formal rulemaking process to consider moving marijuana from a Schedule I to a Schedule III controlled substance.
- STATE DEVELOPMENTS: Maryland became the latest in a growing list of states to adopt pay transparency requirements, the Utah Antidiscrimination Act was amended to expand religious accommodation requirements for employers, and Colorado enacted the nation's first artificial intelligence (AI) law designed to prevent algorithmic discrimination.
- COUNTY DEVELOPMENTS: Lehigh County, Pennsylvania enacted a new and expansive anti-discrimination ordinance that establishes county-specific non-discrimination requirements for employment, housing, education, health care, and public accommodations. The ordinance becomes effective June 1, 2024.
- INTERNATIONAL DEVELOPMENTS: The European Union (EU) Artificial Intelligence (AI) Act that takes effect next month adopts a risk-based approach to regulation whereby AI systems are designated into four categories: Unacceptable Risk, High Risk, Limited Risk, and Minimal Risk. The higher the risk designation, the more restrictive the regulation.

I hope you find the MAY 2024 SCREENING COMPLIANCE UPDATE both entertaining and informative.

Nicolas S. Dufour

ClearStar Executive Vice President, General Counsel & Corporate Secretary

Nicolas Dufour serves as EVP, General Counsel, corporate secretary, data privacy officer, and is a member of the executive management team for ClearStar. He is proficient in the FCRA, GLBA, Data Privacy Framework, and GDPR compliance, as well as other data privacy regimes. He is responsible for managing all legal functions to support the evolving needs of a fast-paced and rapidly changing industry. His position includes providing legal guidance and legal management best practices and operating standards related to the background screening industry, federal, state, and local laws and regulations, legal strategic matters, product development, and managing outside counsels. He represents the company in a broad range of corporate and commercial matters, including commercial transactions, M&A, licensing, regulatory compliance, litigation management, and corporate and board governance. He researches and evaluates all aspects of legal risks associated with growth in to different markets. He assists the management team in setting goals and objectives in the development, implementation, and marketing of new products and services. He also advises and supports management, Board of Directors, and operating personnel on corporate governance, company policies, and regulatory compliance.

FEDERAL DEVELOPMENTS

What Employers Need to Know About the EEOC's New Guidance on Workplace Harassment

Executive Summary: On March 29, 2024, the EEOC announced new guidance addressing harassment in the workplace, which goes into effect immediately. This guidance consolidates the EEOC's previous guidance and incorporates new topics reflecting recent changes in the law. For instance, the Guidance enumerates new categories under "sex-based" harassment, including harassment based upon pregnancy, childbirth, or related medical conditions, including the choice to have or not have an abortion and to use or not use contraception, sexual orientation, and gender identity. Although an earlier attempt at issuing new guidance stalled during the Trump administration, this guidance shows a continued effort to "reflect[] important developments affirming that individuals are protected against harassment on the basis of sexual orientation and gender identity."

Highlights of the New Guidance

The guidance makes clear that the following conduct can form the basis of a harassment claim:

- Intentional use of a name or pronoun inconsistent with the individual's known gender identity (misgendering);
- Denial of access to a bathroom or other sex-segregated facility consistent with the individual's gender identity;
- Disclosing an individual's sexual orientation or gender identity without permission;
- Insulting, criticizing, and demeaning behavior towards a person based on their pregnancy or pregnancy-related medical condition, such as lactation or morning sickness;
- Insulting, criticizing, demeaning, or changing the working conditions of an employee based on their decision to use or not use contraception, including abortion.

The guidance also addresses two concepts that may be unfamiliar to employers—retaliatory harassment and intraclass and intersectional harassment. Retaliatory harassment refers to harassment that occurs when an individual experiences harassment as a result of engaging in protected activity. The guidance also discusses intraclass and intersectional harassment, providing illustrative examples of each. According to the guidance, intraclass age-based harassment would occur when a 52-year-old supervisor directs derogatory comments toward a 65-year-old employee, even though they both are in the protected age category as employees over the age of forty. The guidance finds that intersectional harassment occurs where individuals are targeted based on their membership in more than one protected category, using the example of a male manager making comments to a 51-year-old female worker that she was having a "menopausal moment."

This new guidance, the first in 25 years, also incorporates the realities of the modern workforce by detailing how harassment can occur between remote workers and online. For instance, conduct is considered to be within the work environment if "it is conveyed using work-related communications systems, accounts, devices, or platforms," including official social media accounts, video conferencing technology, and instant messaging system. Employers can also be liable if the conduct occurs in a non-work environment but has an impact on the workplace. This includes posts on social media if the victim learns of the post through a coworker, or if the post otherwise impacts the victim's workplace.

This guidance does not come without its criticisms, and will likely face legal challenges based on, among other grounds, religious discrimination grounds and concerns that it exceeds the scope of the Supreme Court's decision in *Bostock v. Clayton County*, 590 U.S. 644 (2020). When the Commission unveiled a draft in September 2023, a coalition of 20 red state attorneys general argued that the guidance illegally stretches the definition of "sex-based harassment" and that they were ready to take "appropriate legal action" if the EEOC did not address its concerns in the final version. However, employers should not act in reliance on any of the challenges succeeding.

CLICK HERE FOR SOURCE ARTICLE

Congress Passes Bill Prohibiting Sharing or Selling Americans' Sensitive Data to Entities Controlled by Foreign Adversaries

On April 24, 2024, President Biden signed into law H.R. 815, which includes the Protecting Americans' Data from Foreign Adversaries Act of 2024 ("the Act"), a bill that passed the House 414-0 as H.R. 7520 on March 20. The Act is one of several recent actions by the U.S. government to regulate transfers of U.S. personal data for national security reasons, with a particular focus on China. While the ultimate policy objectives are similar, the Act takes a different approach by comparison

to the Biden Administration's Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern ("the EO"), which the U.S. Department of Justice ("DOJ") is in the process of implementing. We summarize below some key features of the Act, which will go into effect on June 23, 2024.

The Act makes it unlawful for data brokers to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual (i.e., people residing in the United States) to any foreign adversary or any entity controlled by a foreign adversary.

- "**Data brokers**" for purposes of the Act are any entity that, for valuable consideration, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available data of United States individuals that the entity did not collect directly from such individuals to another entity. The Act exempts certain entities from the meaning of "data broker." Specifically, the Act does not apply to an entity to the extent that such entity:
    - (i) is transmitting data of a U.S. individual, including communications of such an individual, at the request or direction of such individual;
    - (ii) is providing, maintaining, or offering a product or service with respect to which personally identifiable sensitive data, or access to such data, is not the product or service;
    - (iii) is reporting or publishing news or information concerning local, national, or international events or other matters of public interest;
    - (iv) is reporting, publishing, or otherwise making available news or information that is available to the general public; or
    - (v) is acting as a service provider. A "**service provider**" is an entity that: (A) collects, processes, or transfers data on behalf of, and at the direction of: (i) an individual or entity that is not a foreign adversary country or controlled by a foreign adversary; or (ii) a Federal, State, Tribal, territorial, or local government entity; and (B) receives data from or on behalf of an individual or entity described in subparagraph (A)(i) or a Federal, State, Tribal, territorial, or local government entity.

As noted above, the Act prohibits making available sensitive data of United States individuals to entities or individuals controlled by a foreign adversary.

- **"Foreign adversary countries**" are those specified in 10 U.S.C. § 4872(d)(2), which currently includes the Democratic People's Republic of North Korea, the People's Republic of China, the Russian Federation, and the Islamic Republic of Iran.
- An entity "**controlled by a foreign adversary**" means an individual or entity that is:
    - (A) a foreign person domiciled in, is headquartered in, has its principal place of business in, or is organized under the laws of a foreign adversary country;
    - (B) an entity with respect to which a foreign person or combination of foreign persons described in (A) directly or indirectly own at least a 20 percent stake; or
    - (C) a person subject to the direction or control of a foreign person or entity described in (A) or (B).

The Act includes in its definition of "**sensitive data**" sixteen categories of data plus any data made available by a data broker "for the purpose of identifying the types of data." Categories of sensitive data include government issued identifiers, biometric information, genetic information, and precise geolocation information, among other things. "**Sensitive data**" is considered personally identifiable if it "identifies or is linked or reasonably linkable, alone or in combination with other data, to an individual or a device that identifies or is linked or reasonably linkable to an individual."

Violations of this Act would be enforced by the Federal Trade Commission ("FTC") as violations of an unfair or deceptive act or practice under the FTC Act. It is unclear how the FTC will interpret and enforce the Act, especially in light of ambiguities in the statutory language, the FTC's lack of national security expertise, and the potential overlap with DOJ's authority under the EO.

CLICK HERE FOR SOURCE ARTICLE

DEA Breaks Silence on Reclassification of Marijuana, Proposing Move to Schedule III

After months of anticipation following the U.S. Department of Health and Human Services' recommendation to reschedule marijuana from a Schedule I to a Schedule III controlled substance, we finally have insight into the direction that the U.S. Drug Enforcement Administration (the DEA) will take on the matter. On April 30, 2024, the DEA announced that it will propose to reclassify marijuana as a Schedule III drug, according to reports. The proposal solidifies the federal government's position on the drug's potential for acceptable medical uses in treatment.

The United States federal government regulates drugs through the Controlled Substances Act (21 U.S.C. § 811) (the CSA), which places controlled substances into five categories, or schedules. Marijuana is currently classified as a Schedule I controlled substance under the CSA, subjecting it to the most stringent of controls. A Schedule I controlled substance by definition has a high potential for abuse and has no accepted medical use in the United States, and there is a lack of accepted safety for the use of the drug under medical supervision. Other drugs in Schedule I include heroin and LSD.

The classification of a drug under Schedule I comes with significant implications. Such classification makes it a felony to possess, manufacture, dispense or distribute the drug, and it cannot be legally prescribed for medical use. Furthermore, a drug's placement on Schedule I makes it extremely difficult for researchers to perform scientific studies. The financial implications are also significant. Marijuana's placement on Schedule I means that marijuana businesses cannot take certain federal tax deductions under the Internal Revenue Code Section 280E. In addition, the placement triggers a host of issues for both businesses and banks, making traditional services unobtainable for marijuana businesses, if not simply prohibitively expensive. This is just to name a few of the consequences that may arise from engaging in the marijuana business – and this is still the case despite the fact that most states in the U.S. now permit and regulate marijuana for medical purposes.

Moving marijuana to Schedule III would put it in the same class as other drugs that have accepted medical use and lower potential for abuse, such as ketamine, Tylenol with codeine, and testosterone. Schedule III drugs are available by prescription, subject to FDA prior approval and registration by a DEA-registered pharmacy. However, the reclassification does not mean that marijuana now becomes "legal." State-authorized marijuana programs as they operate today will continue to be illegal, because such dispensaries are not federally approved, and neither are the marijuana products they dispense. Schedule III drugs are still highly regulated, and although penalties for violations are less than that of a Schedule I drug violation, many legal consequences will remain in place even after the rescheduling is finalized. However, the move is still a progressive step that will open doors for further policy reform.

If the rescheduling is ultimately approved, perhaps the most direct and immediate consequence for businesses will be tax relief. Section 280E prohibits the taking of deductions for business that engage in trafficking of controlled substances listed in Schedule I and II. A move to Schedule III means that those marijuana businesses will be eligible to deduct expenses like any other business. This means more profits and increased ability to compete against illegal sellers. Investment and research are likely to increase accordingly.

There are several administrative steps that need to occur before the rescheduling is finalized, and it will likely take many months to complete the rulemaking process. It is anticipated that the move will be hotly contested by opponents, and delays in implementation are to be expected. The uncertainties created by the reclassification will likely take years to shake out.

Disclaimer:
Possessing, using, distributing, and/or selling marijuana or marijuana-based products is illegal under federal law, regardless of any state law that may decriminalize such activity under certain circumstances. Although federal enforcement policy may at times defer to states' laws and not enforce conflicting federal laws, interested businesses and individuals should be aware that compliance with state law in no way assures compliance with federal law, and there is a risk that conflicting federal laws may be enforced in the future. No legal advice we give is intended to provide any guidance or assistance in violating federal law.

CLICK HERE FOR SOURCE ARTICLE

Proposed Marijuana Reclassification and Impact on Employers

On May 16, 2024, the U.S. Department of Justice announced that the Attorney General has submitted a notice of proposed rulemaking initiating a formal rulemaking process to consider moving marijuana from a Schedule I to a Schedule III controlled substance.

Regulatory Next Steps

The rescheduling of a controlled substance follows a formal rulemaking procedure that requires notice to the public, and an opportunity for comment and an administrative hearing. The Attorney General's proposal starts the process, where the Drug Enforcement Administration (DEA) will gather and consider information and views submitted by the public, in order to make a determination about the appropriate schedule. During that process, and until a final rule is published, marijuana remains a Schedule I controlled substance. The Controlled Substances Act, passed in 1970, created five schedules of classifications of various substances, placing cannabis on Schedule I, along with heroin, LSD, and other drugs with "no currently accepted medical use or treatment" value. While reclassifying cannabis would not legalize recreational cannabis nationwide, it would place cannabis with other Schedule III drugs, including ketamine, anabolic steroids, and some acetaminophen-codeine combinations.

Implications for Employers

The DEA proposal has no immediate impact on state or federal laws regulating marijuana. Prospectively, the biggest impact may concern employers in industries, such as transportation, that perform drug testing in accordance with federal requirements. The Federal Omnibus Transportation Employee Testing Act requires all U.S. Department of Transportation (DOT) agencies to implement drug and alcohol testing requirements for "safety-sensitive" employment positions regulated by those agencies. Accordingly, employees with safety-sensitive responsibilities regulated by agencies, including the Federal Aviation Administration, Federal Motor Carrier Safety Administration, and the Federal Railroad Administration, are subject to extensive mandatory drug testing.

Safety-sensitive employees subject to mandatory testing are identified in the regulations promulgated by the various DOT agencies, but generally consist of pilots, school bus drivers, truck drivers, train engineers, subway operators, aircraft maintenance personnel, armed security personnel, ship captains, and pipeline emergency response personnel. Safety-sensitive employees are subject to pre-employment, random, reasonable suspicion, post-accident, return-to-duty, and follow-up drug testing as required and detailed by each agency's governing regulations. The DOT currently requires drug testing for the following five drugs or classes of drugs: (a) marijuana metabolites; (b) cocaine metabolites; (c) amphetamines; (d) opioids; and (e) phencyclidine (PCP). *See* 49 CFR 40.82. The DOT's authority to conduct drug testing of safety-sensitive employees is also derived from the Department of Health and Human Services Mandatory Guidelines for Federal Workplace Drug Testing Programs, which permit regulated employers to test for those drugs listed in Schedule I or II of the Controlled Substances Act.

As the regulatory process unfolds, there will likely be scrutiny placed on identifying those substances to be tested on behalf of the large universe of federally regulated safety-sensitive employees. If marijuana is moved from Schedule I to Schedule III, a classification where medical use is permitted, it remains to be seen whether the DOT would adjust compliance requirements.

CLICK HERE FOR SOURCE ARTICLE

HUD Issues Fair Housing Act Guidance on Applications of Artificial Intelligence

On Friday, May 3, the U.S. Department of Housing and Urban Development (HUD) released two guidance documents addressing the application of the Fair Housing Act to two areas in which the use of artificial intelligence poses particular concerns: the tenant screening process and its application to the advertising of housing opportunities through online platforms that use targeted ads. Today's announcement is in accordance with President Joe Biden's Executive Order, which called on HUD to provide guidance to combat discrimination enabled by automated or algorithmic tools used to make decisions about access to housing and in other real estate-related transactions.

"Under this Administration, HUD is committed to fully enforcing the Fair Housing Act and rooting out all forms of discrimination in housing," **said HUD Acting Secretary Adrianne Todman.** "Today, we have released new guidance to ensure that our partners in the private sector who utilize artificial intelligence and algorithms are aware of how the Fair Housing Act applies to these practices."

"The Fair Housing Act prohibits discrimination on the basis of race, color, national origin, religion, sex (including gender and sexual orientation), disability, and familial status," **said Demetria McCain, Principal Deputy Assistant Secretary Fair Housing and Equal Opportunity**. "Housing providers, tenant screening companies, advertisers, and online platforms should be aware that the Fair Housing Act applies to tenant screening and the advertising of housing, including when artificial intelligence and algorithms are used to perform these functions."
The tenant screening guidance describes fair housing issues created by tenant screening practices, including the increasing use of third-party screening companies to aid with tenant screening decisions and the emerging use of machine learning and artificial intelligence. The guidance also suggests best practices for fair, transparent, and non-discriminatory tenant screening policies, for both housing providers and companies that offer tenant screening services.

The Fair Housing Act prohibits both intentional housing discrimination and housing practices that have an unjustified discriminatory effect. Housing providers and tenant screening companies both have a role to play in ensuring that tenant screenings are transparent, accurate, and fair. The tenant screening guidance makes clear that use of third-party screening companies, including those that use artificial intelligence or other advanced technologies, must comply with the Fair Housing Act, and ensure that all housing applicants are given an equal opportunity to be evaluated on their own merit.

Read the tenant screening guidance here.

Advertisers and online platforms should be alert about the risks of deploying targeting advertisement tools for ads covered by the Fair Housing Act. Violations of the Act may occur when certain ad targeting and delivery functions unlawfully deny consumers information about housing opportunities based on the consumers' protected characteristics. Violations of the Act may also occur when ad targeting and delivery functions are used, on the basis of protected characteristics, to target vulnerable consumers for predatory products or services, display content that could discourage or deter potential consumers, or charge different amounts for delivered advertisements.

Read the guidance for use of online platforms here.

The release of these guidance documents follows HUD's pledge in an April 4 joint statement with other federal agencies to enforce civil rights laws as new technologies like artificial intelligence become more common. HUD's release of the tenant screening guidance also fulfills a commitment HUD made in the Biden-Harris Administration's Blueprint for a Renters Bill of Rights.

CLICK HERE FOR SOURCE ARTICLE

New Guidance for Federal Contractors Using Artificial Intelligence (AI) in Hiring

On April 29, 2024, the OFCCP released a series of FAQs outlining the requirements covered federal contractors must meet when using AI systems for hiring and related employment purposes to ensure they are maintaining compliance with Equal Employment Opportunity (EEO) obligations. Covered federal contractors are obligated by law to ensure that they do not discriminate in employment and that they take affirmative action to ensure employees and applicants are treated without regard to their race, color, religion, sex, sexual orientation, gender identity, national origin, disability, or status as a protected veteran. If not designed and implemented properly, OFCCP warns that AI systems have the potential to embed bias and discrimination into a range of employment decision-making processes.

OFCCP's guidance outlines several affirmative obligations that federal contractors should be aware of, including:

- Maintaining records for resume searches and substantive search criteria—regardless of whether the resume search is from an external website or internal resume database—and ensuring the confidentiality of those records.
- Cooperating with OFCCP by providing the necessary, requested information on AI systems.
- Making reasonable accommodations for known physical or mental limitations of an otherwise qualified applicant or employee with a disability.

The OFCCP's guidance also offers federal contractors some best practices for using AI systems, including providing notice when using AI in the hiring process and ensuring that the AI system interfaces, data inputs, and outputs comply with accessibility standards for people with disabilities.

Additionally, OFCCP clarified that federal contractors are responsible for the use of third-party products and services, such as a staffing agency, HR software provider, or vendor. So, even when using another entity's AI products or services, federal contractors cannot delegate nondiscrimination and affirmative action obligations. As such, federal contractors cannot escape liability for the adverse impact of discriminatory screenings conducted by a third party. OFCCP's guidance discusses the best practices for hiring a vendor-created AI system to be in compliance with EEO obligations and the requirements federal contractors should be able to verify, including:

- the transparency and explainability of the AI system;
- any differences between the data that the AI system was trained, developed, and validated and the contractor's candidate pool or labor market;
- the screening tools and data used to filter in or prioritize candidates, such as job skills or keywords, as well as any data used to filter out candidates with gaps in employment history; and
- the vendor's data protections and privacy policies.

Within its guidance, OFCCP has made it clear that it will be executing evaluations and complaint investigations to ensure federal contractors using AI in their employment decisions are in compliance with nondiscrimination obligations. OFCCP also recently updated its compliance review process to require documentation to better identify discrimination related to AI systems by federal contractors.

Federal contractors considering implementing AI systems for hiring or employment decisions should conduct due diligence on the third party provider of the AI system and use the OFCCP guidance above to evaluate whether or not the AI system is appropriate for use by federal contractors.

CLICK HERE FOR SOURCE ARTICLE

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

Maryland Adopts Pay Transparency Requirements

Maryland has become the latest in a growing list of states to adopt pay transparency requirements, with its governor recently signing the Maryland Wage Range Transparency Act into law.

The new law significantly amends Maryland's Equal Pay for Equal Work Law and will now require employers, regardless of size, to disclose a 1) good faith wage and salary range, 2) a general description of any benefits, and 3) a general description of any other compensation that might be offered in job postings for any work "that will be physically performed, at least in part," in Maryland. If no posting is created, employers must still disclose this information to an applicant upon request, or at any time before a discussion of compensation is had with an applicant.

The law does not specify what qualifies as an appropriate "general description of benefits and any other compensation offered."

Employers should also be mindful of the recordkeeping requirements of the act, which requires employers to maintain records of compliance with the new law for a period of three years from the date the position was filled (or if the position is ultimately not filled, from the date the position was initially posted).

The law will go into effect Oct. 1, 2024. Violations will be subject to enforcement measures by Maryland's Commissioner of Labor and Industry. First violations will be subject to a compliance order, while second violations may result in up to a $300 penalty for each applicant for whom the employer is not in compliance. For each subsequent violation within a three-year period, such penalties escalate to up to $600 per instance of non-compliance.

Following Washington, D.C.'s adoption of similar requirements, along with President Biden's recent announcement requiring pay transparency for federal contractors, Maryland's adoption of pay transparency requirements signals the continuing interest in such legislation across the country. As more states continue to consider and adopt these measures, employers must continue to be attentive to this evolving patchwork of pay transparency requirements.

CLICK HERE FOR SOURCE ARTICLE

New Discrimination Protections in Maryland's Anne Arundel and Montgomery Counties

Employers with employees in Anne Arundel and Montgomery Counties should be aware of developments that increase the protections for employees against discrimination.

In Anne Arundel County, a new, comprehensive discrimination law has been passed that expands the scope of the existing law beyond housing to include employment. Among other things, the protected categories under the law have been extended to cover an employee's "perceived" protected class and their association with someone in a protected class. The law now specifically prohibits retaliation as well. The law also sets up a mechanism for employees to file complaints with the Anne Arundel County Human Rights Commission, with an investigative and hearing process. (This is similar to existing processes in several other counties). Should the Commission find discrimination, however, the remedies are limited to a cease and desist order and a civil fine of up to $5,000 per offense. Moreover, if an employee also files a complaint under federal or state law, the County complaint will terminate.

In Montgomery County, a new law will prohibit all employers with any employees in the County from asking for or seeking healthcare information unless it is necessary to determine if an applicant meets job qualifications that have been published prior to the acceptance of applications. Employers are also prohibited from asking applicants about sexual or reproductive health information, including information related to abortion care, miscarriage, contraception, sterilization, pregnancy, sexually transmitted diseases, fertility treatment, gender affirming care, or family planning. It is worth noting that, under Maryland law, employers may not require applicants to provide health information that is unrelated to the job, while the Americans with Disabilities Act prohibits employers with 15 or more employees from asking disability-related questions of applicants prior to a conditional job offer. The law will take effect on July 26, 2024.

CLICK HERE FOR SOURCE ARTICLE

Maryland Creates a New Paradigm for Data Privacy

Maryland joins the growing list of states to enact a privacy law but adds unique requirements for data minimization, sensitive data, and consumer health data

On May 10, 2024, Maryland Governor Wes Moore signed the Maryland Online Data Privacy Act of 2024 ("MODPA" or the "Act"), bringing the number of comprehensive state privacy laws to 18and establishing a new, more restrictive framework for businesses that collect, process, or disclose personal data. MODPA will become effective on October 1, 2025, but it will not apply to any personal data processing activities before April 1, 2026.

Like other comprehensive state privacy laws, MODPA gives consumers the right to confirm processing of and to access, correct, delete, and port their personal data, as well as the right to opt out of sales of their personal data and the use of such data for targeted advertising or profiling; requires controllers to post privacy policies and conduct data privacy impact assessments; and prohibits controllers from discriminating against consumers who exercise their rights; exempts certain entities and data from the Act entirely;[1] and defines many terms—such as "personal data" and "sale" of personal data—the way that other states have defined them. As explained below, however, MODPA diverges in other important respects from the approach that other states have taken, which will complicate privacy compliance and data use strategies.

Lower Application Thresholds

MODPA applies to entities that conduct business in Maryland or provide products or services that are targeted to residents of the state and that during the preceding calendar year met either of two criteria:

- Controlled or processed the personal data of at least 35,000 consumers (i.e., Maryland residents), excluding personal data controlled or processed solely for the purpose of completing a payment transaction; **or**
- Controlled or processed the personal data of at least 10,000 consumers and derived more than 20 percent of its gross revenue from the sale of personal data.

Most states that are as populous as Maryland have established thresholds of 100,000 or more consumers. Maryland's low threshold, which aligns with the threshold in the Delaware Personal Data Privacy Act (DPDPA), means some entities that can avoid compliance with other states' privacy laws because they collect personal data from under 100,000 state residents will nonetheless need to comply with MODPA.

Different Definitions of Biometric Data, Consumer Health Data, and Sensitive Personal Data

While most of the definitions in MODPA mirror those in the other state privacy laws, several do not. For instance, most state privacy laws limit the definition of "biometric data" to information generated by automatic measurements of biological characteristics that *is used or intended to be used* to *identify*a specific individual. MODPA, however, defines "biometric data" to mean "data generated by automatic measurements of the biological characteristics of a consumer that *canbe used* to uniquely *authenticate* a consumer's identity."[2] (Emphasis added.) Because "biometric data" is "sensitive personal data" under the Act, controllers will have to comply with the strict requirements regarding such data, even if they never intend to use it to authenticate or identify a consumer.

MODPA also regulates "consumer health data," which means "personal data that a controller uses to identify a consumer's physical or mental health *status*," including, but not limited to, "data related to (1) gender affirming care, or (2) reproductive or sexual health care." (Emphasis added.) Other state laws that regulate "consumer health data" have defined the term more narrowly. For instance, the amended Connecticut Data Privacy Act defines the term to mean "personal data that a controller uses to identify a consumer's physical or mental health *condition or diagnosis*," and Washington's My Health My Data Act regulates only data that is "reasonably linkable" to a consumer's health. The definition in MODPA is broader because personal data that identifies an individual's health "status"—as opposed to "condition or diagnosis"—could include aspects of a consumer's health that have nothing to do with a "condition or diagnosis," such as information revealing a consumer's general fitness, nutrition habits, certain purchases, and so forth. Because "consumer health data" is "sensitive personal data," the broad definition will mean that more personal data will be subject to the strict requirements that govern "sensitive personal data."

As noted above, "sensitive personal data" includes "consumer health data," as well as data that reveals race or ethnic origin, religious beliefs, sex life or orientation, status as transgender or nonbinary, citizenship or immigration status, or national origin. Genetic or biometric data are also "sensitive personal data," regardless of whether they are used to identify a specific individual, as is the personal data of a known child under 13 years of age, and precise geolocation data. This definition differs from those in other state privacy laws, most of which do not include data revealing national origin or biometric and genetic data that is not used to identify specific individuals.

First-of-a-Kind Data Minimization Requirements

MODPA establishes data minimization requirements for both personal data and *sensitive* personal data that are more restrictive than those in other state privacy laws and, in some respects, even the EU General Data Protection Regulation ("GDPR"). These obligations will have a significant impact on companies because in some cases, they will prohibit routine business operations that involve personal data. Specifically, MODPA will impose the following:

- **Strict limits on the *processing* of sensitive personal data*, regardless of consumer consent*.** Controllers may not process (i.e., collect, use, disclose, or maintain) sensitive personal data—*regardless of consumer consent*—except when doing so is "strictly necessary" to "provide or maintain a specific product or service requested by the consumer." Controllers therefore will not be able to use precise geolocation for geo-targeted advertisements and may be precluded from using data that reveals race or ethnicity to offer certain demographic groups content that is likely to be of interest to them or information about someone's diet or exercise for advertising. This provision also may prevent controllers from providing enhanced services to consumers if those enhancements require the use of sensitive data (such as precise geolocation information) but are not "strictly necessary" to provide the underlying service. The scope of this prohibition also will depend on how broadly or narrowly the state attorney general and the courts define "specific product or service requested by the consumer."
- **Prohibition on *sales* of sensitive personal data*, regardless of consumer consent.*** Similarly, controllers are prohibited from "selling" sensitive personal data—i.e., exchanging such data for monetary or other valuable consideration—regardless of whether a consumer consents. This will preclude the disclosure of sensitive personal data for purposes that are permissible with consumers' consent under other state laws. Because MODPA exempts *consumer-directed* disclosures from the definition of "sale," however, it may be possible to disclose sensitive personal data to third parties when the consumer has directed the disclosure or intentionally used the controller to interact with the third party. Moreover, controllers will be able to disclose sensitive personal data to third parties when necessary to provide the product or service requested, because such disclosures are also exempt from the definition of "sale."
- **Limitation on *collection* of personal data*, regardless of consumer consent*.** Controllers must "limit the collection of personal data" to what is "reasonably necessary and proportionate" to "provide or maintain a specific product or service requested by the consumer to whom the data pertains," regardless of whether a consumer consents. Controllers have some leeway in determining what is "reasonably necessary and proportionate," but they should document their reasoning so that they can explain to regulators, if necessary.
  Other state privacy laws do not restrict *collection* of personal data—or sensitive personal data—to what is necessary to provide a product or service but, rather, allow controllers to collect such data for purposes that were disclosed to the consumer and—in most states—with consumer consent. For instance, the Virginia Consumer Data Protection Act requires 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*." (Emphasis added.) Connecticut and Colorado take a similar approach, as does California, which expands the minimization requirement to other types of processing—i.e., use, retention, and sharing of personal information.
- **Limitation on *processing* of personal data to what is reasonably necessary for disclosed—or compatible—purposes, *unless the consumer consents*.** Other states have adopted a similar approach to data minimization that allows controllers to process personal data, so long as such processing is reasonably necessary for the purposes that were disclosed to consumers in the privacy policy (or reasonably compatible with such purposes).

No Processing of Minors' Personal Data for Sales or Targeted Advertising

Under MODPA, a "minor" means a Maryland resident whom the controller "knew **or should have known**" is under 18 years of age. This heightened standard (i.e., "should have known" rather than an "actual knowledge" or "willful disregard"

that the consumer was a minor) will require controllers that do business or target consumers in Maryland (and process personal data of the requisite number of consumers) to determine what information puts them on notice that a particular consumer is a minor so that they can avoid "selling" such consumers' data or targeting ads to them. Again, exceptions to the definitions of "sale" and "targeted advertising" may be useful; but regardless of whether exceptions apply in any given circumstance, controllers will need to modify their compliance programs—possibly by adding an age assurance or age verification mechanism—to satisfy this obligation.

Maryland's absolutist approach may be vulnerable to a First Amendment challenge on the grounds that the ban on sales and targeted advertising to teens imposes an impermissible content—and speaker-based restriction on commercial speech.

Obligations Regarding Consumer Health Data

Like several other state privacy laws, MODPA regulates "consumer health data" by prohibiting any person from (1) providing an employee or contractor access to such data unless that individual is subject to a contractual duty of confidentiality; (2) providing a processor access to consumer health data unless the controller and processor adhere to the obligations that controllers have under the Act; (3) using a geofence to identify, track, or collect data from—or send notifications to—a consumer within 1,750 feet of a health-care facility regarding the consumer's health data; or (4) selling or offering to sell consumer health data without the consumer's consent.

These obligations will create significant compliance challenges. For instance, the requirement to obtain consumers' consent before "selling" consumer health data conflicts with the blanket prohibition against sales of sensitive personal data (which is defined to *include* consumer health data) *regardless of consumer consent*, and it is not clear how controllers are expected to reconcile these two obligations, other than to apply the most restrictive provision. Moreover, controllers that are subject to other state laws—e.g., the Connecticut Data Privacy Act—that govern consumer health data will not be able to rely on the policies and procedures that they have implemented to comply with those laws because MODPA defines "consumer health data" more broadly and imposes greater restrictions on the processing of "sensitive personal data" (which includes "consumer health data").

Data Protection Assessments for Processing That Presents a Heightened Risk of Harm

Controllers must conduct and document on a regular basis a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer, including an assessment for each algorithm that is used. Unlike other state privacy laws, MODPA limits the scope of processing activities that presents a "heightened risk of harm" to the following: (1) targeted advertising; (2) sales of personal data; (3) processing sensitive personal data; and (4) processing personal data for profiling that presents certain types of reasonably foreseeable risks—i.e., unfair, abusive, or deceptive treatment; disparate impact; financial, physical, or reputational injury; physical or other intrusion on the solitude or seclusion or private affairs or concerns, when it would be offensive to a reasonable person; or other substantial injury. What is different—and more expansive—is the requirement to conduct an assessment for "each algorithm" that the controller uses, although regulations implementing the Colorado Privacy Act require controllers to conduct a data protection assessment when the level of risk for a particular processing activity increases, and they include the use of an algorithm as something that could increase risk.

Consumers' Rights

As noted above, MODPA gives consumers the right to confirm the processing of their personal data, as well as to request access to and correction, deletion, and export of their personal data. Regarding opt-out rights, controllers have discretion to recognize universal opt-out signals that consumers use to opt out of sales, targeted advertising, or profiling, but they are not required to do so. Like the Oregon Consumer Privacy Act, MODPA requires controllers to provide consumers with a list of the categories of third parties to which that particular consumer's personal data has been disclosed or, if that is not possible, a list of categories of third parties to which the controller has disclosed *any* consumer's personal data.
Like other state privacy laws, MODPA prohibits controllers from discriminating against consumers for exercising their rights. Unlike other state privacy laws, MODPA prohibits controllers from collecting, processing, or transferring personal data *or publicly available information* in a manner that has an unlawful discriminatory impact on the equal enjoyment of goods and services on the basis of protected characteristics (e.g., race), unless this different treatment is due to certain permissible purposes, such as to diversify an applicant pool. Other state privacy laws prohibit processing personal data in

a way that is unlawful under antidiscrimination laws, but they do not regulate the use of publicly available information in this manner.

Notice to Consumers

MODPA requires controllers to provide consumers with a privacy notice that explains, among other things, the personal data collected, for what purpose the personal data is collected, and the categories of third parties to whom the controller discloses personal data. The Act also requires third parties that use or share a consumer's "information" to provide the consumer with notice of any new or changed practice that is inconsistent with the representation made to the consumer at the time the data was collected. It is not clear whether third parties could rely on the controller to provide this notice. Presumably, third parties could obligate controllers to do so in their agreements with controllers but, ultimately, third parties will be responsible for ensuring that consumers receive this notice.

Exceptions

MODPA provides the usual exceptions for processing personal data necessary to comply with applicable law, to protect cybersecurity and prevent fraud, and so forth. Unlike other state privacy laws, however, MODPA does not provide an exception for internal processing of personal data for product and service development or improvement. It does allow controllers and processors to "[p]erform internal operations that are (1) reasonably aligned with the expectations of the consumer or can be reasonably anticipated based on the consumer's existing relationship with the controller or (2) otherwise compatible with processing in furtherance of (a) the provision of a product or service specifically requested by a consumer, or (b) the performance of a contract to which a consumer is a party." It may be possible to argue that the internal use of personal data for product development and improvement fits into this category.

Enforcement and Sunset Provisions

The Maryland attorney general and the Division of Consumer Protection have exclusive enforcement authority. With respect to an alleged violation on or before April 1, 2027, the attorney general must give controllers and processors sixty days to cure an alleged violation after receiving notice. If the controller or processor fails to cure the alleged violation within sixty days, the attorney general may initiate an enforcement action under Maryland Consumer Protection Act ("MCPA") and may collect up to $10,000 per violation (and up to $25,000 per subsequent violation). While MODPA states that consumers are not prohibited from pursuing any other remedy under law, it does make clear that consumers may not bring a private right of action under the MCPA. It does not state that the criminal penalties available for violations of the MCPA will not apply, however.

CLICK HERE FOR SOURCE ARTICLE

Employers Face June 1, 2024 Deadline to Comply with Lehigh County, Pennsylvania's New Expansive Anti-Discrimination Ordinance

The Lehigh County Human Relations Ordinance was enacted February 26, 2024, establishing county-specific non-discrimination requirements for employment, housing, education, health care and public accommodations. The ordinance also creates a Lehigh County Human Relations Commission charged with investigating and enforcing claims of discrimination. The ordinance becomes effective June 1, 2024.

Expanded Protected Characteristics and Employer Coverage

With respect to employment, the ordinance establishes the following protected characteristics, some of which exceed present federal law protections: race, ethnicity, color, religion, creed, national origin or citizenship status, ancestry, sex (including pregnancy, childbirth, breastfeeding, and related medical conditions), gender identity, gender expression, sexual orientation, genetic information, marital status, familial status, earning a GED rather than high school diploma, physical or mental disability, relationship or association with a disabled person, source of income, age, height, weight, veteran status, use of guide or support animals and/or mechanical aids, or domestic or sexual violence victim status. Importantly, the ordinance protects both "actual" and "perceived" protected characteristics. It also expressly prevents employers from denying employment because of a "prior disability."

Unlike Title VII or Pennsylvania state law, any "person or organization" who employs even a ***single employee*** is covered by the law.

Prohibitions Relating to Criminal Record History and Salary History

The ordinance follows recent nationwide trends relating to use of criminal history and salary history in employment. Specifically, employers may not:

- Ask, on an employment application, whether the applicant has ever been convicted of a crime;
- Require a job applicant to disclose prior criminal convictions until after an initial interview;
- Consider conviction records that do not relate to an applicant's suitability for employment; or
- Ask a job applicant what their salary is or was from any current or previous employment.

The law specifically prohibits "[e]licit[ing] any information or mak[ing] or keep[ing] a record of, or us[ing] any form of application or application blank, containing questions or entries concerning the protected class of any applicant for employment." This resembles recently enacted laws around the country that, for instance, prohibit employers from requiring applicants to disclose age on employment applications.

Remedial Provisions

If an employee believes an employer has violated any provision of the ordinance, they can file a verified complaint with the Lehigh County Human Relations Commission (created by the ordinance), within 180 days of the alleged act of discrimination, similar to the process currently before the Pennsylvania Human Relations Commission. The ordinance also provides for a private right of action if the Commission dismisses the complaint, or a year passes after filing of the complaint.

Recommendations

Pennsylvania employers with operations in Lehigh County should review and if necessary revise application materials and hiring procedures to comply with the new ordinance. This is particularly important with respect to the ordinance's prohibitions that exceed state law, such as the restrictions on use of certain application questions and restrictions related to criminal record and salary history. Employers should also familiarize themselves with the significantly expanded list of protected characteristics under the law and consider training programs to ensure compliance when making employment decisions.

CLICK HERE FOR SOURCE ARTICLE

Utah Expands Employee Religious Protections

The Utah Antidiscrimination Act has been amended to expand religious accommodation requirements for employers under Utah law.

The Utah Legislature passed House Bill 396 (H.B. 396), and Governor Spencer Cox signed the bill on March 19, 2024. The new law will go into effect on May 1, 2024.

Currently, Section 112 of the Utah Antidiscrimination Act requires employers to allow employees to express "religious or moral beliefs and commitments in the workplace" as long as they do so in a "reasonable, non-disruptive, and non-harassing way." Section 112 also prohibits retaliation against employees who express religious beliefs outside the workplace "unless the expression is in direct conflict with the essential business-related interests of the employer."

H.B. 396 expands Section 112's workplace protections by prohibiting employers from making employees engage in "religiously objectionable expression" that the employee reasonably believes would burden or offend the "employee's sincerely held religious beliefs." H.B. 396's definition of "religiously objectionable expression" is much broader than mere speech. Under the bill, "religiously objectionable expression" means "expression, action or inaction that burdens or offends a sincerely held religious belief, including dress and grooming requirements, speech, scheduling, prayer, and abstention, including abstentions relating to healthcare."

Under H.B. 396, employees who believe they are being required to engage in "religiously objectionable expression" may request an accommodation. The employer must not compel the employee to engage in the religiously objectionable expression unless the accommodation would cause an "undue burden" to the employer. H.B. 396 defines an "undue burden" as something that substantially interferes with the employer's "core mission" or the employer's "ability to conduct business in an effective or financially reasonable manner." The accommodation also cannot substantially interfere with the employer's "ability to provide training and safety instruction for the job." Employers with fewer than 15 employees are not required to provide scheduling accommodations under the law.

Now would be an excellent time for Utah employers to evaluate their current religious accommodation procedures for compliance with both state law and the U.S. Supreme Court's interpretation of employers' obligations under Title VII of the Civil Rights Act in *Groff v. DeJoy*.

CLICK HERE FOR SOURCE ARTICLE

Nebraska Enacts Comprehensive State Privacy Law

On April 17, 2024, Governor Jim Pillen signed into law a bill (L.B. 1074) enacting the Nebraska Data Privacy Act ("NEDPA"). The NEDPA will take effect on January 1, 2025.

Applicability

The NEDPA is similar in structure and scope to the Texas Data Privacy and Security Act. The NEDPA applies solely to persons that: (1) conduct business in Nebraska or produce a product or service consumed by residents of Nebraska; (2) process or engage in the sale of personal data; and (3) are not small businesses as determined under the federal Small Business Act, except to the extent that provisions limiting the sale of sensitive data apply.

The NEDPA applies to Nebraska consumers (i.e., Nebraska residents who act only in an individual or household context and not in a commercial or employment context). The NEDPA also contains a number of exemptions, including for financial institutions, affiliates of a financial institution, or data subject to Title V of the Gramm-Leach-Bliley Act; covered entities or business associates under HIPAA; nonprofit organizations; institutions of higher education; suppliers of electricity; and natural gas public utilities.

Controller Obligations

Similar to other comprehensive state privacy laws, the NEDPA requires 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 need a consumer's consent to process sensitive data or to process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer. The NEDPA also requires controllers to establish, implement and maintain reasonable administrative, technical and physical data security practices that are appropriate to the volume and nature of the personal data at issue.

The NEDPA also requires controllers to provide a reasonably accessible and clear privacy notice that includes: (1) the categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller; (2) the purpose for processing personal data; (3) how a consumer may exercise a consumer right, including the process by which a consumer may appeal a controller's decision with regard to the consumer's request; (4) if applicable, any category of personal data that the controller shares with any third party; (5) if applicable, any category of third party with whom the controller shares personal data; and (6) a description of each method required through which a consumer may submit a request to exercise a consumer right.

The NEDPA also requires a controller to conduct and document a data protection assessment of each of the following processing activities involving personal data:

- the processing of personal data for purposes of targeted advertising;
- the sale of personal data;

- the processing of personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of: (1) unfair or deceptive treatment of or unlawful disparate impact on any consumer; (2) financial, physical or reputational injury to any consumer; (3) a physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of any consumer, if the intrusion would be offensive to a reasonable person; or (4) other substantial injury to any consumer;
- the processing of sensitive data; and
- any processing activity that involves personal data that presents a heightened risk of harm to any consumer.

Consumer Rights

The NEDPA provides consumers with rights to: (1) confirm whether a controller is processing the consumer's personal data and to access the personal data; (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data; (3) delete personal data provided by or obtained about the consumer; (4) if the data is available in a digital format and the processing is completed by automated means, obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance; and (5) opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.

Like many of the other state privacy laws, controllers have 45 days to respond to consumer rights requests, with a potential 45-day extension when reasonably necessary.

Enforcement

The NEDPA does not contain a private right of action and will be enforced exclusively by the Nebraska Attorney General. The NEDPA provides a 30-day cure period that also requires: (1) a written statement that the controller or processor cured the alleged violation and supportive documentation to show how such violation was cured; and (2) an express written statement that the controller or processor shall not commit any such violation after the alleged violation has been cured. The cure provision does not expire.

Effective Date

The NEDPA will take effect on January 1, 2025.

CLICK HERE FOR SOURCE ARTICLE

"AI Bias Audits and Emerging Risks When Using AI for Hiring & Employment," AI Across Industries

On July 5, 2023, a first-of-its-kind law went into effect in New York City that mandated annual bias audits of AI-enabled systems (NYC LL 144). As the 2024 reporting deadline approaches, have you thought about your organization's reporting or how you'll proactively conduct these audits?

In this webinar, KC Halm (Co-Chair, DWT's AI Team), Matt Jedreski (Counsel, DWT's Employment Group), Paul White (Partner, Resolution Economics, LLC), and Gurkan Ay (Director, Resolution Economics, LLC) discuss the broader legal landscape (i.e. what other regulations have emerged since NYC LL 144 went into effect). They also dive into what these AI audits will look like practically, and methodological considerations for gathering the necessary data and conducting an effective AI bias audit.

CLICK HERE FOR SOURCE ARTICLE

Colorado Enacts Nation's First AI Discrimination Law

On May 17, Colorado's governor signed the nation's first artificial intelligence law designed to prevent algorithmic discrimination. The law is slated to go into effect on February 1, 2026.

The Colorado Artificial Intelligence Act ("CAIA") requires companies that develop and use "high-risk" AI systems to use reasonable care to protect consumers from algorithmic discrimination. Supporters of the legislation state the CAIA is needed to protect against discriminatory biases that may be inherent in certain AI technologies. Here are some key provisions of the law:

- The law impacts "high risk" AI systems. According to the law, a "high-risk" AI system is one that makes, or is a substantial factor in making, a decision regarding a financial or lending service, insurance, housing, employment, education enrollment, health care, government services, or legal services.
- Applies to users and developers. Notably, the CAIA applies to companies that use AI technologies as well as those that develop it.
- Reasonable care requirement. The CAIA will require companies to use "reasonable care" to protect consumers from "any known or reasonably foreseeable risks of algorithmic discrimination."
- Notice requirements. The law requires that companies report any discovery of algorithmic discrimination to the state attorney general. In addition, developers of high-risk artificial intelligence systems must disclose to the Colorado attorney general and to all known deployers or other developers of the high-risk AI system any known or reasonably foreseeable risks of algorithmic discrimination arising from the intended uses of the high-risk artificial intelligence system.
- Risk management policies. Any company that uses a high-risk AI system must implement a risk management policy to govern the deployment of high-risk AI systems. In addition, companies will be required to mitigate known or reasonably foreseeable risks of algorithmic discrimination.

Despite signing this legislation into law, Governor Polis released a signing statement expressing reservations with the bill. Polis noted that while the law generally focuses on prohibiting intentional discriminatory conduct, it "deviates from that practice by regulating the results of AI system use, regardless of intent." Polis encouraged the legislature to reexamine this law before it is finalized and takes effect in 2026.

CLICK HERE FOR SOURCE ARTICLE

COURT CASES

Hostile Work Environment Harassment May Be Based on Disability

Employees may bring a hostile work environment claim arising from disability, according to the U.S. Court of Appeals for the Ninth Circuit. Although this was the first time the Ninth Circuit addressed the issue, it joined a number of sister Circuits that had previously recognized such a claim.

In *Mattioda v. Nelson*, the employee had disabilities that required him to travel in a premium class for flights over an hour. He alleged that, after he reported his disabilities and requested travel accommodations, he was subjected to derogatory comments from his supervisors, who also inhibited his work opportunities, gave him unwarranted negative job reviews, and resisted his accommodation requests. The employee eventually sued for violations of the Rehabilitation Act (which is the analog to the Americans with Disabilities Act for federally-funded programs), claiming, among other things, that he had been subjected to hostile work environment harassment based on his disability.

Until this case, the Ninth Circuit had not yet decided whether harassment claims could be brought under the Rehab Act or the ADA. But here, the Ninth Circuit found that they could, observing that it was joining "the weight of consensus" by all sister Circuits previously addressing the issue (the Second, Fourth, Fifth, Eighth and Tenth; the First, Third, Ninth, Eleventh and D.C. Circuits have assumed without deciding that such claims are possible). As these other Circuits had reasoned, the ADA uses almost identical language to Title VII, under which hostile environment harassment claims have long been recognized.

This case reminds employers that employees can bring hostile work environment claims based on disability, in addition to the more commonly asserted bases under Title VII of race, sex, religion and national origin. It is critically important that employers respond promptly and effectively to employee complaints of harassment, regardless of the basis.

CLICK HERE FOR SOURCE ARTICLE

An Employee Using Marijuana Is Not Protected Under the ADA

Although many states have legalized the use of medical and/or recreational marijuana, it still remains an illegal drug under federal law – and the U.S. Court of Appeals for the Sixth Circuit recently held that a marijuana user was therefore not protected by the Americans with Disabilities Act.

In *Maxson v. Baldwin*, an employee with a back injury was admittedly addicted to prescription medications and alcohol, and also used marijuana to reduce the pain. Shortly after showing up for work with withdrawal symptoms that interfered with his ability to do his job, he was terminated for a positive marijuana test, as well as an arrest and misdemeanor guilty plea for attempting to obtain dangerous drugs. He sued, arguing that the true reason for his termination was his addiction to prescription drugs and alcohol.

Under the ADA, alcoholism is considered to be a disability (although employers may still hold alcoholic employees accountable for meeting performance and conduct standards). However, as the Sixth Circuit noted, the ADA provides that an employee who is "currently engaging in the illegal use of drugs" is not entitled to the protections of the law. According to EEOC guidance, drug use is current if it "occurred recently enough to justify an employer's reasonable belief that involvement with drugs is an on-going problem." Here, the Sixth Circuit found sufficient evidence of current drug use in the employee's admitted use of marijuana, the positive marijuana test, and the withdrawal symptoms. Accordingly, the employee was excluded from coverage under the ADA.

Employers should be aware, however, that even though the ADA will not protect medical marijuana users, the EEOC may still require them to engage in an interactive process with the employee to ascertain if other accommodations may be available based on the employee's underlying disability. In addition, there may be employment protections for medical (and even recreational) marijuana users under state law.

CLICK HERE FOR SOURCE ARTICLE

EEOC's New Guidance on Workplace Harassment Being Challenged

In its first update since 1999, the Equal Employment Opportunity Commission (EEOC) recently published updated enforcement guidance on workplace harassment. The 189-page guidance, which consolidates and replaces five previous guidance documents issued from 1987 through 1999, clarifies the EEOC's position on various types of harassment, incorporates new developments in the law, most notably those relating to LGBTQ+ employee rights, and addresses circumstances in modern society such as electronic communications, social media and remote work. The guidance also includes numerous hypothetical examples illustrating harassment against individuals in each protected classification under federal discrimination laws. The guidance was published on April 29. By May 13, a lawsuit challenging the guidance was filed.

Below are some highlights of the EEOC's guidance and the current legal challenge to it.

LGBTQ+ Rights

One of the most noteworthy changes in the EEOC's guidance relates to LGBTQ+ employee rights. This change was a result of the Supreme Court's 2020 decision in *Bostock v. Clayton County*, which held that discriminating against an employee based on gender identity or sexual orientation is unlawful sex discrimination under Title VII. The EEOC's guidance defines sex-based discrimination under Title VII to include "repeated and intentional use of a name or pronoun inconsistent with the individual's known gender identity (misgendering) or the denial of access to a bathroom or other sex-segregated facility consistent with the individual's gender identity." The EEOC noted that *Bostock*'s reasoning about the nature of discrimination based on sex "logically extends to claims of harassment." Examples of harassment based on sexual orientation or gender identity include epithets, physical assault, disclosing an individual's sexual orientation or gender identity without permission, and harassing conduct because an individual presents themselves in a way that is different than the stereotype associated with that person's sex.

Pregnancy, Childbirth and Related Conditions

The EEOC's guidance makes clear that conduct based on an individual's pregnancy, childbirth or related medical conditions, such as using or not using contraception, or choices regarding abortions, falls under the umbrella of sex-based discrimination and harassment. Examples include negative comments about an employee's ability to work due to morning sickness or inappropriate conduct toward a lactating employee.

Color

The EEOC's guidance separated out color harassment from that relating to race and national origin, clarifying that "[a]lthough sometimes related to harassment based on race or national origin, color-based harassment due to an individual's pigmentation, complexion, or skin shade or tone is independently covered by Title VII." Harassment based on color could include specific comments made about the color of one's skin, as well as harassment of groups of employees of the same race based on their complexion when others of the same race who have a different complexion are not harassed.

Intraclass and Intersectional Harassment

The guidance illustrates different types of harassment. "Intraclass" harassment occurs when both the harasser and the individual being harassed are in the same protected category. For example, someone in their 50s could harass someone in their 60s by making ageist comments even though both are older than 40 and age protected.

"Intersectional" harassment occurs when an individual is harassed because that person is a member of more than one protected category. For example, the harassment of a Black woman based on stereotypes about Black women would constitute both race and sex harassment.

Recognizing Current Circumstances

The EEOC's guidance recognizes some differences in society since the last guidance was issued more than 25 years ago. It makes clear that even if certain conduct (such as "electronic communications using private phones, computers or social

media accounts") does not occur in a work-related context, it can nonetheless impact the workplace and affect terms and conditions of employment. Given the growth of technology, the guidance emphasizes that "it is increasingly likely that the non-consensual distribution of real or computer-generated intimate images, such as through social media, messaging applications, or other electronic means, can contribute to a hostile work environment, if it impacts the workplace." Further, since its guidance is the first update since the COVID-19 pandemic, the EEOC explained that the guidance applies to remote work locations as well.

The Legal Challenge

Despite the EEOC's efforts to address the approximately 38,000 comments received during the comment period before it issued the final rule on May 13, 18 states filed a lawsuit in Tennessee federal court, claiming the guidance unlawfully expands transgender rights under Title VII beyond the Supreme Court's decision in *Bostock*, including on such issues as pronouns and bathroom use. That same court vacated the EEOC's June 2021 guidance relating to sexual orientation and gender identity.

Given the legal challenge, the status of the EEOC's guidance is unclear at this point. Employers should remember, however, that state and local law may provide even greater protections to employees than those under Title VII or the EEOC's guidance. Further, employers are encouraged to ensure that their policies effectively address issues in the modern workplace, including harassment in the contexts of the remote workplace and social media. Employers are also encouraged to confer with employment counsel to ensure that they comply with the law applicable to their workplaces.

CLICK HERE FOR SOURCE ARTICLE

INTERNATIONAL DEVELOPMENTS

EU Artificial Intelligence Regulations Take Effect Next Month

The AI Act adopts a risk-based approach to regulation. AI systems are designated into four categories: Unacceptable Risk, High Risk, Limited Risk, and Minimal Risk. The higher the risk designation, the more restrictive the regulation. For example, "unacceptable" uses, such as using AI to assess the risk of an individual committing criminal offenses (think *Minority Report*), are strictly prohibited; however, minimal risk uses, such as an email provider's spam filter, are unregulated. The table below outlines how each risk level is categorized and the regulatory requirements for providers of such AI systems.

Risk Level	Use Examples	Regulatory Requirements	AI Act Reference
Unacceptable	Social scoring systems; "manipulative" AI systems or programs; compilation of facial recognition databases; inferring emotions in workplaces or educational institutions; assessing risk of an individual committing criminal offenses; exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behavior.	Strictly prohibited.	Title II, Article 5.
High	Use impacts health, safety, or fundamental rights of a natural person; critical infrastructure; education; employment; migration; democracy; elections; rule of law; the environment.	Establish a risk management system. Conduct data governance of system inputs and outputs. Design system for record-keeping. Provide instructions for use. Implement human oversight. Design system to achieve appropriate levels of accuracy, robustness, and security. Establish a quality management system to ensure compliance. Register AI system in the EU database established under the AI Act.	Title III, Articles 6 and 8-15.

Limited	Chatbots, shallow-fake and deep-fake generation.	Ensure end-users are on notice that they are interacting with AI.	Recitals 53 and 134 – 137.
Minimal	AI-enabled games, spam filters, automated.	Unregulated.	N/A.

General purpose AI (GPAI) models and systems could fall into any of the four categories of risk. GPAI systems used as high risk AI systems or integrated into them will require providers to take additional steps. For example, providers of GPAI models must:

- Document training, testing, and evaluation results.
- Provide downstream providers with information and documentation so that providers understand the capabilities and limitations of integrating the GPAI model into the downstream provider's AI system.
- Adhere to internal policy devoted to honoring the Copyright Directive.
- Publish a detailed summary of the content used for training.

In addition, all GPAI models with systemic risk must track, document, and report incidents and possible corrective measures to the EU AI Office, and relevant national competent authorities without "undue delay." Such incidents may include instances where the AI system generates discriminatory results or inadvertent manipulative content.

As a result of the AI Act, AI providers looking to offer services in the EU will be required to prepare for and satisfy bias testing to identify algorithmic discrimination with their systems. For providers focused on offering products and services in the United States, the requirements set forth under the AI Act offer a strong preview of what can be expected for future federal or state legislation. For example, earlier this month, the Colorado General Assembly passed SB24-205, which sets forth consumer protections for AI and follows a similar risk-based approach. The bill was signed into law on May 17, 2024, and takes effect Feb. 1, 2026.

In the coming days, the AI Act will be published in the EU bloc's Official Journal of the European Union and will take effect 20 days after publication. Although implementation will largely be conducted in phases, many regulations will take effect next month.

CLICK HERE FOR SOURCE ARTICLE

MISCELLANEOUS DEVELOPMENTS

Terminating Workers in the Private Sector for Their Political Affiliations and Activities

As this year's political campaigns heat up and elections draw closer, heated discussions in hallways, postings on social media platforms, and expressing support for candidates tend to become all too common in the workplace. When these activities begin to affect workplace productivity and morale, private employers may wonder if they can fire employees based on their political affiliation and activities. In many cases, they can, since there is no federal law that prohibits discrimination based on political affiliation or beliefs.

Unlike government workers, who have protections under the First Amendment for their political behavior outside the workplace, private workers do not enjoy any legal protections of their political speech and activities. The only exception for employees of private companies is under selected state laws and local ordinances, which may offer protection, at least to varying degrees.

For instance, a few states prohibit political affiliation discrimination by private companies, including California, Louisiana, Missouri, New Mexico, South Carolina, Utah, and Washington D.C. Significantly more states ban discrimination based on political activities, but these laws often provide very limited protections that apply only in certain situations. For example, the laws in Georgia and Ohio only provide protection for employees if an employer tries to intimidate them into voting a certain way or not voting at all. Likewise, the New York law very narrowly defines political activity, so many actions by employees may not fall within the protections of the law.

In other situations, an employee's actions may be protected as political activity, but it also may violate other employer policies or rules if it occurs in the workplace. For instance, if political activity interferes with employee performance, violates prohibitions on personal or mass email messages, or breaches rules on employee attire at work, the employee may face discipline for other reasons.

On the federal level, employers may not prevent employees from engaging in concerted activities to impact legislation, such as minimum wage increase or other similar policies. Doing so may cause employers to run afoul of the National Labor Relations Act. Employers also must take care not to take any disciplinary action that could be construed as violating Title VII of the Civil Rights Act of 1964, which prevent discrimination based on various protected classes, including race, sex, gender, religion, or national origin.

Whether state or local laws impact an employer's ability to terminate workers based on political affiliation or activity or not, employers should consider the other consequences of doing so. Some employees may welcome employer action to rid the workplace of a highly offensive person. However, other employees may believe that employers should stay out of employees' personal business and allow them to have their own political opinions. Therefore, taking disciplinary action in this situation could either boost or lower employee morale in general, depending on the circumstances.

CLICK HERE FOR SOURCE ARTICLE