AUGUST 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

TABLE OF CONTENTS

SCREENING COMPLIANCE UPDATE | AUGUST 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

August 2024 Screening Compliance Update Executive Summary

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

- FEDERAL DEVELOPMENTS: Although a recent Department of Transportation (DOT) final rule approved oral fluid drug testing as an alternative for workers regulated by the Federal Motor Carrier Safety Administration, Federal Aviation Administration, Federal Railroad Administration, and Federal Transit Administration, its use as an alternative to urine testing has been delayed and remains in flux.
- STATE DEVELOPMENTS: In August 2024, Illinois Governor J.B. Pritzker signed into law a bill related to Artificial Intelligence (AI) which protects employees against discrimination from the use of AI in employment-related decisions. Illinois also passed a state law offering protection to employees from unfair enforcement of Employment Verification practices.
- INTERNATIONAL DEVELOPMENTS: The Privacy Commissioner of Canada, the Information and Privacy Commissioner for British Columbia, and the Information and Privacy Commissioner of Alberta announced a joint investigation into the privacy compliance of a Canadian company that offers tenant screening services in Canada.

I hope you find the AUGUST 2024 SCREENING COMPLIANCE UPDATE both informative and helpful in keeping up with establishing and maintaining a compliant background screening program.

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

Swiss-US Data Privacy Framework: Adequacy Decision for Certified US Companies

The Swiss Federal Council has decided on 14 August 2024 that the new Swiss-US Data Privacy Framework (DPF) allows for the secure exchange of personal data between Switzerland and certified US companies and, as a result, issued an adequacy decision for the US in this respect. The certification for US companies will allow personal data to be transferred from Switzerland to certified companies in the US without additional safeguards. The DPF presents a significant relief for Swiss companies sharing personal data with US recipients and puts Switzerland at level with the EU/EEA and the UK where such a framework had already been implemented more than one year ago.

The Swiss-US Data Privacy Framework in a Nutshell and its Implications

Under the Federal Act on Data Protection (**FADP**), in force since 1 September 2023, personal data may be transferred abroad without additional safeguards only if the recipient country has an adequate level of data protection. The Federal Council decides which jurisdictions meet this requirement and has published a binding list of these countries in Annex 1 to the Data Protection Ordinance (**DPO**). If a country is not listed, the international data transfer is only permissible if additional safeguards are put in place (e.g. the EU Standard Contractual Clauses with the necessary amendments for Switzerland and transfer impact assessments) or if an exemption applies (e.g. the data subject's consent) (Art. 16, 17 FADP). Until now, the Federal Council did not deem the US to provide for an adequate level of data protection and the US was thus not listed in Annex 1 to the DPO.

The DPF was developed by the US Department of Commerce and the Swiss Federal Administration to provide reliable and compliant mechanisms for personal data transfers from Switzerland to the US. This is achieved by a certification mechanism – US companies can certify themselves under the DPF. The certification ensures that the required data protection measures and data protection guarantees are observed and put in place. In particular, the US companies are only permitted to process personal data for the purposes for which they were initially collected. Disclosure to third parties such as to non-certified companies is not permitted. In the event of access by US authorities to personal data transferred from Switzerland various safeguards are provided, including access to a redress mechanism.

Therefore, the Federal Council concluded that the DPF allows for the secure exchange of personal data between Switzerland and certified US companies, approved the corresponding amendment to the DPO at its meeting of 14 August 2024 and added the US in this context to the list of countries with adequate data protection.

What's Next and How Does This Impact You?

The amendment of the DPO will become effective on 15 September 2024. From this date, you may transfer personal data to certified US companies without having to implement additional guarantees or to rely on a statutory exemption. The US companies currently certified are listed here.

For data transfers to non-certified US companies, safeguards such as Standard Contractual Clauses and transfer impact assessments will remain necessary. We also recommend maintaining as a fallback any pre-existing safeguards put in place for certified US companies since certifications and the DPF altogether may eventually be challenged and invalidated.

CLICK HERE FOR SOURCE ARTICLE

Cannabis Rescheduling: Closing of the Comment Period and What Lies Ahead

The proposed rescheduling of cannabis from Schedule I to Schedule III under the Controlled Substances Act (CSA) marks a pivotal moment in the evolution of U.S. cannabis policy but may bring few practical changes to state-licensed markets. On May 20, the U.S. Department of Justice (DOJ) and the Drug Enforcement Administration (DEA) issued a Notice of Proposed Rulemaking[1] (NPRM) to initiate the change, launching a 60-day public comment period that concluded on July 22. The proposal has stirred significant interest and debate among stakeholders, including state regulators, advocacy groups, health experts, individuals, and licensed businesses, resulting in the posting of more than 43,000 comments.

This article will explore the diverse spectrum of public comments on the proposed rule, the evolving understanding of the implications of moving cannabis to Schedule III, and the procedural steps that may lie ahead in the rulemaking process.

Closing of the Comment Period

The 60-day public comment period for the proposed rescheduling rule officially closed on July 22. The DOJ received approximately 43,000 comments, about 17% of which (approximately 7,500 comments) were submitted in the final three days.[2] A wide array of stakeholders, including state regulators, advocacy and opposition groups, health experts, and patients, all voiced their perspectives on the proposal, reflecting the complex and multifaceted nature of cannabis policy in the U.S.

Among the pro-reform advocates, an analysis by the Drug Policy Alliance (DPA) shows that a majority of commentors believe that rescheduling cannabis to Schedule III would not go far enough in addressing the federal prohibition's broader implications.[3] The DPA found that 69% of commentors supported the complete descheduling of cannabis from the CSA, as opposed to rescheduling to Schedule III. The DPA's analysis also revealed that a substantial portion of the comments emphasized the need for federal marijuana reform to advance racial justice and social equity.

Public comments from state regulatory agencies also highlighted a need for clarity on how rescheduling would impact state-legal recreational cannabis markets. The NPRM specifically states that "[i]f marijuana is transferred into Schedule III, the manufacture, distribution, dispensing, and possession of marijuana would remain subject to the applicable criminal prohibitions of the CSA." This statement has led to uncertainty about the practical implications of rescheduling for existing state markets.

For instance, in addition to comments submitted by the Cannabis Regulators Association in July,[4] the Michigan Cannabis Regulatory Agency (CRA) submitted comments providing information on the state's medical program in support of the finding that cannabis does have a currently accepted medical use in treatment in the U.S., and stressed the importance of federal guidance on the implications of rescheduling in several key areas, including the applicable general requirements for Schedule III substances, banking and taxation, bankruptcy protections, product packaging, labeling, advertising, and safety standards, transportation and interstate commerce, research, and federal enforcement priorities and regulatory agencies. The CRA's executive director stated that "the CRA wanted to make it very clear in our public comment that rescheduling will do little good if the federal government fails to provide clear and robust whole-of-government guidance on the implications of the rescheduling."[5]

Implications of Moving Cannabis to Schedule III

While the move to Schedule III is seen by many as a positive step toward recognizing the medical benefits of cannabis, it is important to understand that rescheduling alone would bring about only limited changes to the current legal and regulatory landscape. One of the most immediate and tangible benefits of rescheduling is the potential tax relief for businesses. Under the current Schedule I classification, the industry is subject to 26 U.S.C. § 280E, which prohibits cannabis businesses from claiming tax deductions for ordinary business expenses such as salaries, rent, and utilities. This prohibition results in a significantly higher effective tax rate when compared to businesses in other industries. Moving cannabis to Schedule III would remove this prohibition, allowing cannabis businesses to deduct these normal business expenses. This change should not be overlooked, as it could provide substantial financial relief to the industry, improving profitability and encouraging further investment and growth.

Beyond the potential tax benefits, the rescheduling of cannabis to Schedule III would bring about few changes in the broader legal framework governing cannabis.[6] As yet another example of this point, a recent report by the Congressional Research Service (CRS) highlights that many of the significant legal conflicts between federal and state cannabis laws would remain unresolved under Schedule III. The report states that cannabis activities not conducted under a valid prescription would continue to be subject to federal criminal penalties.[7] This means that the cultivation, distribution, and possession of cannabis for recreational use would continue to violate federal law, maintaining the status quo for state-legal recreational markets.

One notable change identified in the CRS report pertains to advertising. Under the current Schedule I classification, traditional advertising for cannabis and cannabis products is prohibited under 21 U.S.C. § 843(C). If cannabis is rescheduled

to Schedule III, this restriction would no longer apply, potentially allowing cannabis businesses to engage in marketing and advertising activities that have historically been restricted. This could lead to an increase in visibility and consumer awareness of cannabis products.

The limitations of rescheduling highlight the need for comprehensive federal legislation to address the broader issues facing the cannabis industry.

Next Steps in the Rescheduling Process

With the close of the public comment period, the rescheduling process moves into a critical phase. The DEA is now tasked with reviewing the public comments and finalizing the rescheduling rule. The DEA will analyze the feedback received during the comment period and may incorporate changes based on new data or arguments presented by stakeholders. The role of the DEA administrator is crucial at this stage, as they will ultimately sign off on the final rule, as well as any administrative hearings on the rule. Opponents have called for,[8] and the DEA may choose to hold, such administrative hearings to gather additional input before the rule is finalized.

The public comments on the proposed rule will likely play a significant role in shaping the final rule. The federal Administrative Procedure Act requires that the DEA consider all relevant material presented during the comment period and "base its reasoning and conclusions on the rulemaking record, consisting of the comments, scientific data, expert opinions, and facts accumulated during the pre-rule and proposed rule stages."[9] The DEA will need to address significant issues raised in the comments and provide a reasoned explanation for its decisions. This process ensures that the final rule is grounded in a thorough consideration of public input and scientific evidence.

Once the DEA completes its review, the final rule will be published in the Federal Register. Typically, a final rule becomes effective 30 days after publication. However, for "significant" and "major" rules, this period may extend to 60 days to allow for further review and compliance planning.[10] The rule's effective date may be subject to delays if legal challenges arise or if the DEA decides to reopen the comment period based on new information.

Opponents of cannabis rescheduling are likely to challenge the final rule in court. These challenges may argue that the rescheduling decision was arbitrary, capricious, or not supported by substantial evidence. The court will evaluate whether the DEA adhered to procedural requirements, considered all relevant factors, and provided a rational basis for its decision. If a court finds that the DEA failed to meet these standards, it may vacate the rule and remand it back to DEA for further consideration. Legal battles could delay the implementation of the final rule and result in further uncertainty for the cannabis industry.

Why It Matters

The proposed rescheduling of cannabis from Schedule I to Schedule III under the CSA represents a significant yet limited step forward in the evolution of federal cannabis policy. The public comment period on the proposed rule brought forth a diverse array of perspectives, with the majority advocating for more comprehensive reforms beyond rescheduling. While tax relief for cannabis businesses is a notable benefit, many of the broader legal and regulatory conflicts between federal and state laws would remain unresolved under Schedule III. The most recent CRS report on rescheduling underscores this point. As the DOJ and DEA proceed with the administrative process, including potential hearings and the finalization of the rule, stakeholders must stay informed and actively engaged.

CLICK HERE FOR SOURCE ARTICLE

Preventing Harassment in the Construction Industry

ABSTRACT: Harassment in the construction industry is a key focus of the EEOC's strategic enforcement plan. Its "Promising Practices" provide employers guidance to preventing and responding to harassment.

The EEOC has recently published its Promising Practices For Preventing Harassment In The Construction Industry to aid employers in addressing and preventing harassment based on race, sex, national origin, or other protected characteristics. Rather than having the force of law, rule, or regulation, the Promising Practices reflects the EEOC's experience with

practices it has found to be effective in preventing harassment. The Promising Practices do not constitute a "safe harbor" from liability for employers who put them into practice, but implementing and applying these practices can help to perfect available affirmative defenses, curry favor with judges and juries deciding harassment cases, and most importantly, potentially prevent harassment in the first place.

The practices identify five core principles the EEOC finds effectively address harassment:

- Committed and engaged leadership;
- Consistent and demonstrated accountability;
- Strong and comprehensive harassment policies;
- Trusted and accessible complaint procedures; and
- Regular, interactive training tailored to the audience and the organization.

Application of these principles has many benefits. Studies show workplaces replete with harassment have higher levels of turnover, higher rates of workplace injuries, lost productivity, and greater difficulty attracting high quality talent. Juries are unlikely to punish employers who are trying to prevent and combat harassment, even if their efforts fall short. Conversely, unengaged or passive leadership and policies that go unenforced are likely to draw their ire.

Importantly, these principles closely track the Faragher-Ellerth affirmative defense under Title VII, which is also applied in many states. An employer is completely relieved of liability for supervisor harassment that does not end in tangible employment action if it can show that: (1) the employer exercised reasonable care to prevent and promptly correct any sexually harassing behavior and (2) that the employee unreasonably failed to take advantage of preventive or corrective opportunities. Engaged leadership that holds harassers accountable under its policies, provides robust and anonymous reporting procedures, and conducts regular training can feel more confident in resisting potential legal claims. The Promising Practices, if adopted, very likely satisfy the "reasonable care" prong of Faragher-Ellerth. An employee probably also acts unreasonably if effective reporting channels exist but he or she fails to utilize them.

Risk Factors

In discrimination and harassment cases, courts frequently look at the totality of the workplace and workforce demographics for evidence that raises an inference of discrimination or unfair treatment. Certain factors not only raise the risk that harassment will occur, but also may be circumstantial evidence of discriminatory intent, lack of reasonable care in preventing harassment, or failure to adequately respond to complaints of harassment.

The risk factors identified by the EEOC include: (1) a homogenous workforce; (2) workplaces where employees are pressured to conform to stereotypes; (3) decentralized workplace; (4) multiple employers present; and (5) project-based workplaces.

General Contractors Should Lead the Way

Promising Practices identifies general contractors as being uniquely positioned to coordinate preventative measures on job sites with multiple employers. If subcontractors do not have the resources to implement and enforce anti-harassment policies, general contractors may be able to step in. In recent years, both the EEOC and NLRB have sought to greatly expand their "joint employer" rules, so general contractors have additional incentives to prevent and correct harassment. The EEOC suggests that a "no wrong door" system, whereby all subcontractors are required to re-route harassment complaints to the appropriate channels, may be appropriate where many subs are present on-site.

Remedying Complaints

In most instances, the subject of the harassment simply wants the harassment to stop. Few employees are looking to set up a discrimination lawsuit, but every complaint and investigation should be treated with the requisite seriousness as if a lawsuit may one day result. That includes adequate record-keeping, interviews with all parties and witnesses, a thoughtful response, and meaningful actions that are likely to end the harassment.

Transferring one of the involved employees may seem tempting. If the subject is separated from the harasser, then problem solved, right? Not necessarily. While courts have previously held that separating a harasser from the subject can be an

effective response, that may no longer be the case. In an important development from this past Supreme Court term, the Court clarified that a claimant does not need to show significant harm, only some harm, to state a discrimination or retaliation claim. As discussed in a previous post on this blog, a transfer without any change in pay or benefits can suffice to state a claim under Title VII. In the construction industry, there are frequently differences in prestige among different assignments, even within the same trade or same project. In an industry in which it is difficult to distinguish oneself, particularly for women, seemingly minor changes to the terms and conditions of employment can have large consequences. A re-assignment, even with the same pay, hours, and benefits, constitutes an adverse employment action if it is viewed as a less favorable path for advancement, training opportunities, or prestige.

The Role of Unions

Collective bargaining agreements regularly include terms such as rates of pay, hours, and on construction projects, jurisdictions for particular bargaining units and union members. An oft-overlooked provision present in most CBAs is a nondiscrimination provision, which typically prohibits discrimination in application of the terms and conditions of employment. This has been interpreted to include harassment and discrimination on the basis of a protected characteristic and is frequently the source of a claim for breach of the union's duty of fair representation (which exists whether there is a non-discrimination clause or not).

Although not usually the designated channel for reporting harassment, union stewards are frequently employees' first contact when problems arise. Union stewards can assist employees in identifying reporting channels and encouraging reporting of inappropriate conduct.

What deference will Courts afford to the Promising Practices?

In light of the recent Supreme Court decision in Loper Bright Enterprises v.Raimondo, which overturned the Chevron doctrine, many may be wondering about whether courts will follow EEOC guidance in harassment suits. The Promising Practices do not have the force of law, but the EEOC's authority to issue educational materials is enshrined in the original text of Title VII, as part of the EEOC's statutory purpose of providing education to employers and prevention of unlawful discrimination in employment. Courts are free to reject any portion of the Promising Practices that may be an "interpretation" of Title VII's terms. However, Courts regularly look to EEOC policy guidance and publications to determine whether an employer has put in place effective and reasonable policies and procedures to address harassment and discrimination. Loper Bright is very unlikely to change that.

CLICK HERE FOR SOURCE ARTICLE

DOT Oral Fluid Drug Testing in a Holding Pattern

Although oral fluid drug testing has been federally approved for truck drivers and workers in safety-sensitive transportation positions, its use as an alternative to urine testing has been delayed and remains in flux.

A Substance Abuse and Mental Health Services Administration official on July 29 told *Safety+Health* that the agency is considering applications filed this spring by three laboratories for certification in oral fluid testing, a benchmark for implementing employer testing.

A recent Department of Transportation final rule approved oral fluid drug testing as an alternative for workers regulated by the Federal Motor Carrier Safety Administration, Federal Aviation Administration, Federal Railroad Administration and Federal Transit Administration.

For employers to enact oral fluid testing, however, HHS must certify at least two laboratories.

“There are currently no laboratories certified to conduct oral fluid drug testing,” the SAMHSA official said, adding that the certification process is ongoing and typically takes three to six months from the receipt of application.

In the final rule, DOT says oral fluid testing “will give employers a choice that will help combat employee cheating on urine

drug tests and provide a less intrusive means of achieving the safety goals" of the department's drug and alcohol testing program.

On June 21, DOT published a direct final rule that would have revised the 2023 rule by:

- Providing temporary qualification requirements for mock oral fluid monitors.
- Providing for consistent privacy requirements by identifying which individuals may be present during an oral fluid collection.
- Clarifying how collectors are to specify that a sufficient volume of oral fluid was collected.

The rule was set to go into effect Aug. 5, but the agency withdrew it on Aug. 1, citing adverse comment from stakeholders.

One such piece of feedback, from the National Drug and Alcohol Screening Association, states that "delaying collector training until after laboratories are HHS-certified will cause small businesses that have met the train-the-trainer course requirements to suffer the loss of training revenue."

The association continues, "It also will create a shortage of properly trained and qualified oral fluid collectors from being able to collect specimens for possibly months after the first laboratories are certified."

FMCSA now will consider comments through a parallel proposed rule – also published June 21.

"The proposed rule invited comment on the substance of these rule changes," the agency says. "DOT will respond to comments as part of any final action taken on the parallel proposed rule."

CLICK HERE FOR SOURCE ARTICLE

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

Illinois Enacts New AI Legislation, Joining Colorado as the Only States Regulating Algorithmic Discrimination in Private Sector Use of AI Systems (US)

2024 has been a historic year in the United States for state legislation aimed at protecting employees from harm arising out of the use of artificial intelligence ("AI") systems. In May, Colorado passed the first US law addressing algorithmic discrimination in private sector use of AI systems, imposing obligations on Colorado employers such as disclosing their use of AI to employees and applicants. Last week, Illinois joined the ranks, imposing new obligations on Illinois employers that use AI systems to make, or that are used to aid in making, employment decisions.

Illinois HB 3773: What Employers Need to Know

On August 9, Illinois Governor J.B. Pritzker signed into law several AI-related bills, including HB 3773 ("HB 3773" or the "Act"), which amends the Illinois Human Rights Act to protect employees against discrimination from, and require transparency about, the use of AI in employment-related decisions. (The other bills address non-employment related issues arising from the use of AI.)

Under HB 3773, an employer cannot use AI that has the effect of subjecting employees to discrimination based on a protected class with respect to, *e.g.*, recruitment, hiring, promotion, discharge, discipline, or the terms, privileges, or conditions of employment. In addition, the Act prohibits employers from using zip codes as a proxy for protected classes. Illinois employers must notify employees of the use of AI to make or aid in making employment-related decisions. HB 3773 applies to any person employing one or more employees within Illinois.

The Act defines "artificial intelligence" as a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, recommendations, or decisions that can influence physical or virtual environments. "Artificial intelligence" is also defined to include "generative artificial intelligence," meaning an automated computing system that, when prompted with human input, can produce outputs that simulate human-produced content such as essays, images, or video.

As with other allegations of employment-related civil rights violations, an employee alleging a violation of the AI provisions in HB 3773 must first file a complaint with the Illinois Department of Human Rights (the "IDHR"). Within 100 days of the filing of the charge, the IDHR will determine if there is substantial evidence to support that the alleged civil rights violation occurred. If not, the charge will be dismissed, but the aggrieved party can seek review of the dismissal before the Illinois Human Rights Commission (the "Commission"). The IDHR must file a complaint with the Commission when it determines there is substantial evidence that the alleged violation occurred. When a complaint is filed with the Commission, any party may elect to have the claim decided in an Illinois circuit court within 20 days after receiving service of the complaint. Available remedies include actual damages, civil penalties ranging from $16,000 to $70,000, attorneys' fees, compliance reporting obligations, and any other action as may be necessary to make the complainant whole.

How Does HB 3773 Differ From Colorado's Artificial Intelligence Act?

Colorado's Artificial Intelligence Act ("CAIA"), structured more as a consumer-protection law, imposes a duty of care on creators and deployers of high-risk AI systems to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination. CAIA does not exclusively regulate employers. Rather, high-risk AI systems include AI systems that make, or assist in making, employment-related decisions. Under CAIA, Colorado employers also must complete annual impact assessments, provide various notices to employees, and implement a risk-management policy and program. Substantially similar to CAIA is HB 5322, a pending Illinois bill that includes affirmative reporting obligations and annual assessments for "deployers" of AI systems, which includes, but is not limited to, employers.

By contrast, HB 3773 amends Illinois' Human Rights Act to make algorithmic discrimination an actionable civil rights violation. In other words, HB 3773 allows Illinois employees to seek relief under the state's Human Rights Act for discrimination arising from their employer's use of an AI system. Unlike Colorado's CAIA, the Act does not require affirmative action from an employer to assess, report, or mitigate the risks arising from the use of AI systems.

As we previously reported, legislation aimed at addressing algorithmic discrimination is pending in multiple states and there are indications that issues arising from the use of AI systems also are being considered at the federal level.

Colorado and Illinois are currently the only US jurisdictions that regulate an employer's use of AI systems. However, all US employers should take note of how regulation at the federal level and at the state level could impact their use of an AI system.

CLICK HERE FOR SOURCE ARTICLE

Illinois Passes State Law Offering Protection to Employees from Unfair Enforcement of Employment Verification Practices

On August 9, 2024, Illinois Governor JB Pritzker signed Senate Bill 0508 ("SB0508") into law. This new law provides additional employment protections for individuals flagged by an employment eligibility verification system, including federal E-Verify, as having identification discrepancies. The new rights and protections created by SB0508 will take effect on January 1, 2025.

In May of 2023, the state amended its Illinois Right to Privacy in the Workplace Act to mandate a specified process employers need to follow if they choose to take an adverse employment action against an employee after receiving notice from an employment eligibility verification system of a discrepancy between an employee's name and social security number. The May 2023 amendment also granted employees certain rights and protections if any such discrepancies arose.

On the heels of this prior amendment, SB0508 clarifies an employee's rights in the event of an E-Verify "no match." The new law will prevent employers from imposing work authorization verification requirements that are greater than those required by federal law. If an employer asserts that a discrepancy exists in an employee's employment verification information, the employer is obligated to provide the employee with certain notices. These notices include the following requirements:

- Providing the employee with the specific document(s) that the employer deems to be deficient, the reason for deficiency, and upon request by the employee, the employer must give the employee the original document forming the basis for the deficiency within seven business days, and would require employers to give employees time to correct documentation discrepancies;
- Instructions on how the employee may correct the alleged deficiencies, if required to do so by law;
- An explanation of the employee's right to have representation present during related meetings, discussions, or proceedings with the employer, if allowed by a memorandum of understanding concerning the federal E-Verify system; and
- An explanation of any other rights the employee may have in connect with the alleged discrepancies.

In addition to providing these notices, SB0508 also affords employees additional rights and protections when an employer receives notification from any federal or state agency of a discrepancy in relation to work authorization. These rights and protections include the following:

- The employer must not take any adverse action against the employee based on notification of discrepancy;
- The employer must provide a notice to the employee as soon as practicable, but not more than five business days after the date of receipt of the notification, unless a shorter timeline is provided for under federal law or a collective bargaining agreement. The notice must include an explanation of the state or federal agency's notification of discrepancy and the time period the employee has to contest the determination from the federal or state agency.
- The employee may have a representative of the employee's choosing in any meetings, discussions, or proceedings with the employer.

SB0508 also provides new provisions that require employers to provide notice to each current employee, by posting in English and in any language commonly used in the workplace, of any inspections of I-9 Employment Eligibility Verification forms or other employment records conducted by the inspecting entity within 72 hours after receiving notice of the inspection. The posted notice shall contain the following details:

- The name of the entity conducting the inspections of I-9 Employment Eligibility Verification forms or other employment records;

- The date that the employer received notice of the inspection; and
- The nature of the inspection to the extent known by the employer; and a copy of the notice received by the employer.

The new law makes an important note that if during an inspection of the employer's I-9 forms by an inspecting entity, the inspecting entity makes a determination that the employee's work authorization documents do not establish that the employee is authorized to work in the United States and provides the employer with notice of that determination, the employer shall provide a written notice to the employee within five business days, unless a shorter timeline is provided for under federal law or a collective bargaining agreement.

This provision requires the employer to notify the employee in person and deliver the notification by hand, if possible, or in the alternative, by mail and email, if the email address of the employee is known. The employer's notice to the employee shall contain the following information:

- An explanation that the inspecting entity has determined that the employee's work authorization documents presented by the employee do not appear to be valid or reasonably relate to the employee;
- The time period for the employee to notify the employer whether the employee is contesting or not contesting the determination by the inspecting entity;
- If known by the employer, the time and date of any meeting with the employer and employee or with the inspecting entity and employee related to the correction of the inspecting entity's determination that the employee's work authorization documents presented by the employee do not appear to be valid or reasonably related to the employee; and
- Notice that the employee has the right to representation during any meeting scheduled with the employer and the inspecting entity.

In the event an employee contests the determination, the employer is to notify the employee within 72 hours of receipt of any final determination from the inspecting agency regarding the employee's work authorization.
It is critical for employers to be mindful of these new provisions as a violation opens the door for an employee or applicant for employment to commence action to enforce these provisions. If the employee or applicant prevails in court, they shall be awarded actual damages plus costs along with additional monetary penalties for willful and knowing violations.

CLICK HERE FOR SOURCE ARTICLE

County of Los Angeles Enacts Fair Chance Ordinance New Hiring Requirements for Employers

What is this about?
On February 27, 2024, the County of Los Angeles Board of Supervisors voted to adopt the County's Fair Chance Ordinance for Employers (FCO). The FCO aligns with the California Fair Chance Act (FCA), also known as "Ban the Box." However, it adds several compliance requirements when considering the applicant's criminal record history to make an employment decision.

Effective Date:
The FCO is operative on September 3, 2024.

Who must comply:
The FCO applies to any "employer" located or doing business in the unincorporated areas of Los Angeles County who ***employs five or more employees regardless of location***. The FCO protects both applicants seeking employment and employees seeking promotions, as well as others seeking non-traditional employment, such as contract or freelance work.

New requirements: Notice of Intent to Conduct Background Check.
This notice must be given along with any conditional offer of employment to the applicant or employee that states (1) the conditional offer is contingent upon a review of a criminal record history and (2) the employer has ***good cause*** to conduct the criminal history review *"**for the specific job position with supporting justification in writing**."* It is not enough for the employer to merely state it reviews such information because of a generalized "safety concern." Specific information is required.

Before employers can take any adverse action against an individual, such as rescinding a conditional job offer, the FCO requires the employer to (1) prepare a ***written individualized assessment*** of an applicant's criminal history in the manner required by the FCO; (2) provide a form of ***preliminary notice of adverse action*** with mandatory content; (3) provide a ***second written individualized assessment*** if the individual provides information in response to the preliminary notice of adverse action; and (4) provide a ***final notice of adverse action*** if the employer makes a final decision to withdraw the conditional offer of employment or take any other adverse action (the final notice must also include mandatory content).

Why compliance matters:
The FCO authorizes public and private remedies, including civil claims. The County of Los Angeles Department of Consumer and Business Affairs (DCBA) is authorized to take appropriate steps to enforce the FCO and conduct investigations of possible violations by an employer. The DCBA may issue monetary penalties of up to $5,000 for the first violation, up to $10,000 for the second violation, and up to $20,000 for the third and subsequent violations.

CLICK HERE FOR SOURCE ARTICLE

Massachusetts Requires Pay Range Disclosure and Pay Data Reporting

On July 31, 2024, Massachusetts Governor Maura T. Healey made it official – with the goal of closing existing wage gaps, Massachusetts is the latest state to require employers to disclose pay range information.

Joining almost a dozen other states that require some form of pay range disclosure (including neighbors Connecticut and Rhode Island), Massachusetts will soon require covered employers to disclose pay range information in job postings and to current employees in certain circumstances. The new law also requires covered employers to submit EEO-1 pay data annually to the Secretary of the Commonwealth.

Effective Dates

Employers will have some time to get ready for these new requirements:

Date	Covered Employer	Obligation
February 1, 2025	Employers with 100 or more employees in Massachusetts and subject to federal EEO filing requirements	Submit demographic and pay data to the Secretary of the Commonwealth
July 31, 2025	Employers with 25 or more employees in Massachusetts	Pay range disclosure obligations go into effect

Pay Range Posting and Disclosure Requirements

Employers with 25 employees or more in Massachusetts are required to:

- Disclose the pay range for a specific position in the job posting.
- Provide the pay range for a specific position to an employee who is offered a promotion or transfer to a new position with different job responsibilities.
- Upon request, provide the pay range for a specific position to an employee holding such position or an applicant for the position.

"Pay range" means "the annual salary range or hourly wage range that the covered employer reasonably and in good faith expects to pay for such position at that time [of posting or disclosure]." Notably, and unlike similar laws in other states (e.g., Maryland), the new law does not require disclosure of other anticipated forms of compensation (e.g., bonuses, commissions)

or other benefits.

"Posting" includes "any advertisement or job posting intended to recruit job applicants for a particular and specific employment position, including, but not limited to, recruitment done directly by a covered employer or indirectly through a third party."

Pay Data Reporting Requirements

The new law also imposes certain pay data reporting obligations on employers that: (a) have 100 or more employees in Massachusetts at any time during the prior calendar year, and (b) are subject to the federal filing requirements of a wage data report.

Covered employers are required to submit to the Secretary of the Commonwealth an EEO data report that includes workforce "demographic and pay data categorized by race, ethnicity, sex, and job category." Submission of a properly completed federal EEO-1 Employer Information Report will satisfy this filing requirement.

Employers must submit this data to the Secretary of the Commonwealth annually by February 1. If applicable, covered employers are also required to submit EEO-3, -4, or -5 data biannually. The Secretary will provide this information to the Massachusetts Executive Office of Labor and Workforce Development for the publication of aggregated data on its website by July 1 of each year.

Importantly, the law specifically clarifies that individual employer reports in the custody of the Secretary of Labor and Workforce Development will ***not*** be considered "public records" subject to disclosure under the Massachusetts Public Records Law. However, this data may be discoverable in litigation.

No Retaliation

Covered employers are prohibited from discharging or in any other manner retaliating or discriminating against an employee or applicant because the employee or applicant has:

- Taken action to enforce their rights pursuant to the law.
- Made a complaint to their employer, the employer's agent, or the attorney general regarding an alleged violation of the law.
- Instituted, or caused to be instituted, any proceeding under the law.
- Testified or is about to testify in any such proceeding.

Enforcement

The attorney general's office has "exclusive jurisdiction" to enforce the law, and may seek declaratory or injunctive relief and impose fines for failing to post or disclose pay range information as requested or failing to submit EEO reports.

- First violations will be subject to a warning.
- Second offenses are subject to a fine of not more than $500.
- Third offenses are subject to a fine of not more than $1,000.
- Fourth or subsequent offenses are subject to civil fines of $7,500 to $25,000 per violation, depending on the circumstances.

Notably, the law does not include a private right of action for applicants or employees against their employers. This is a significant departure from pay disclosure laws in other states (e.g., Washington) where aggrieved employees can bring an action against their employer in court for injunctive relief or damages. Of course, employees already have several sources of protection under federal and state law if they believe they are being discriminated against in their pay.

Also, the law specifically clarifies that violations are not subject to treble damages under the Massachusetts Wage Act.

Next Steps for Covered Employers

While many employers have already begun sharing pay range information in job postings, it is much less common at this

point for employers to share pay range information upon the request of a current employee. To prepare for this new requirement, we encourage all employers with 25 or more employees in Massachusetts to take the following steps ***before*** July 31, 2025:

- Carefully review your current process for setting pay rates as well as your current job titles. This is a good time to evaluate whether any changes are needed.
- Carefully analyze your current pay data to ensure there are no pay equity issues. Employers with 100 or more employees should also consider conducting a full pay equity audit to identify any concerns. As always, we recommend doing so under the attorney-client privilege.
- Consult with employment counsel to address any issues that surface in your analysis of current pay data or your pay equity audit.
- Finally, multistate employers should develop a compliance strategy for dealing with potentially differing pay disclosure requirements.

Fortunately, Massachusetts employers have time to prepare for these new obligations. That time will go quickly, however, so we encourage employers to get started soon to ensure that things are in good order come February 1 and July 31, 2025.

CLICK HERE FOR SOURCE ARTICLE

Renters in Montgomery County Gain New Protections from Background Check Discrimination

The Montgomery County Council unanimously passed legislation last week to amend the county's current "Ban the Box" law and clarify renters' rights when a landlord performs background and credit checks.

Bill 8-24, Human Rights and Civil Liberties – Fair Criminal History and Credit Screenings – Amendments (PDF), introduced by Councilmember Laurie-Anne Sayles and co-sponsored by Councilmembers Evan Glass and Sidney Katz, aims to ensure that tenants are aware of their rights when seeking to rent a home.

The legislation passed 10-0, with Councilmember Dawn Luedtke absent, according to MCM.

"I appreciate Councilmember Glass and Councilmember Katz for their efforts in passing the Housing Justice Act in 2021, which prohibits a housing provider from conducting a criminal background check or credit history during the rental application process before making an offer for rent to a prospective tenant," Sayles said last week. "Despite the bill's implementation in 2021, there were concerns regarding its enforcement and accountability. Bill 8-24 addresses these concerns by adding two new full-time employees to the Office of Human Rights to support enforcement and accountability measures."

"Ban the Box" laws, also known as the Housing Justice Act of 2021, aim to end discrimination against formerly incarcerated people by prohibiting landlords from conducting criminal background or credit checks before making an offer to a prospective tenant.

Under the new law, landlords and apartment complexes will be required to prominently display information about the county Housing Justice Act on their websites and in rental offices. Additionally, the bill mandates landlords to post notices about the use of criminal history in rental housing decisions, report specific disaggregated data on rental applications annually, retain rental application supplements for a certain period, and certify receipt of a completed criminal and credit screening addendum as part of the annual rental housing survey.

According to MCM, the new law prohibits landlords from requesting information about an arrest record that did not lead to a conviction. They also cannot inquire about an arrest record or conviction related to specific offenses such as trespassing, misdemeanor theft, failure to leave public buildings or grounds, indecent exposure, public urination, violating the open container law, marijuana possession, a first conviction for disturbance of the peace or disorderly conduct, or a motor vehicle violation.

Additionally, the new legislation will result in the creation of two new full-time positions at the county's Office of Human Rights.

When introducing the bill in March, Sayles told MoCo360 last week that she decided to draft the bill after a resident contacted her office to complain about a rental application denial.

"When my staff asked who was responsible for receiving these complaints, there was a bit of confusion about where that responsibility lies," Sayles said, noting that the county's Office of Human Rights is responsible for processing such complaints.

Sayles said that she collaborated with its staff to create the new regulation.

"Today, the Council took another step toward correcting decades of unjust housing policies," Councilmember Glass said last week. "This bill strengthens the protections outlined in the Housing Justice Act, which I spearheaded in 2021 as the Lead for Homelessness and Vulnerable Communities. To create a more equitable Montgomery County, we must ensure that residents who have experienced homelessness or minor offenses are not discriminated against when finding a place to live."

In addition to the new rental background check regulations, the Council passed two other key laws affecting renters in July, including rent stabilization and new tenant safety regulations prompted by a deadly fire at the Arrive Silver Spring apartment complex last year.

CLICK HERE FOR SOURCE ARTICLE

Impact of Ohio Legal Recreational Marijuana on Employers

In November 2023, Ohio passed a recreational marijuana law. Sales of recreational marijuana began on August 6 in the Buckeye State, and employers can expect an uptick in employee use.

Employers' rights with respect to marijuana use are unaffected by the new law. Employers are not:

- Required to permit or accommodate an employee's use, possession, or distribution of marijuana; nor
- Prohibited from refusing to hire, discharging, disciplining, or otherwise taking an adverse action against an individual because of the individual's use, possession, or distribution of marijuana.

This is true even if an individual's marijuana use is lawful and off-duty. The new law does not create a cause of action for employees or applicants based on any such action by an employer. Employers in Ohio can continue enforcing drug testing policies, drug-free workplace policies, and zero-tolerance drug policies.

Employers that continue to prohibit marijuana use and plan to test for it may want to remind employees of the company's policy, requirements, and expectations. Among other things, Ohio employers should ensure their drug and alcohol policies clearly state that:

- Marijuana may not be used during work time, including during meal breaks and rest breaks; and
- Marijuana impairment during work time will not be tolerated.

It is also a good time to reevaluate drug policies to determine whether they are tailored to the needs of the business and consistent with both state and federal law.

CLICK HERE FOR SOURCE ARTICLE

COURT CASES

Connecticut Adopts Narrow Definition of "Supervisor" for Hostile Work Environment Claims

The Connecticut Supreme Court recently adopted the U.S. Supreme Court's relatively narrow definition of "supervisor" for use in determining when employers are liable under the Connecticut Fair Employment Practices Act (CFEPA) for creating or failing to remedy a hostile work environment. The decision provides employers with clarity as the term is not defined by the CFEPA.

How We Got Here

In *O'Reggio v. Commission on Human Rights and Opportunities*, SC20847 (Aug. 1, 2024), the plaintiff had worked as an adjudicator for the Connecticut Department of Labor. She sued the department claiming the program service coordinator to whom she reported had subjected her to a hostile work environment. The program service coordinator had authority to assign the plaintiff work, approve leave requests, set schedules, provide training and conduct reviews. The program service coordinator did not have authority, however, to hire, fire or discipline the plaintiff or other employees.

The trial court and, on an initial appeal, the Connecticut Appellate Court found the program service coordinator was not a supervisor as that term was defined by the U.S. Supreme Court in *Vance v. Ball State University*, 570 U.S. 421 (2013). Consequently, those Connecticut courts ruled, the department was not automatically liable for the program service coordinator's alleged acts.

In her appeal to the Connecticut Supreme Court, the plaintiff argued that the *Vance* definition of supervisor was too narrow for use in hostile work environment claims under the CFEPA. She urged the court to hold that the program service coordinator exercised sufficient control over employee working conditions to render the employer liable for abuse of such "supervisory" power.

The Decision

In a 4-3 decision, the Connecticut Supreme Court narrowly rejected the approach advocated by the plaintiff. Instead, the court adopted the *Vance* guidelines for determining which supervisors' actions will result in employer liability. Under the federal statutes considered in *Vance*, an employer will be held vicariously liable for a hostile work environment created by the conduct of supervisors, unless it can satisfy the so-called *Faragher/Ellerth* affirmative defense. In simple terms, the employer must show that it took reasonable steps to forbid and prevent harassment, announced and maintained a procedure for receiving complaints and, when it learned of harassment, remedied it promptly and effectively. Conversely, if the employee creating a hostile work environment is a co-worker, a plaintiff must meet a higher, negligence standard to impute liability to the employer. It is, therefore, important to distinguish between supervisors and coworkers.

In *Vance*, the U.S. Supreme Court determined that for the purpose of hostile work environment claims under federal law, a supervisor is "an employee empowered by the employer 'to take tangible employment actions against the victim, *i.e.*, to effect a significant change in employment status such as hiring, firing, failing to promote, reassigning with significantly different responsibilities, or causing a significant change in benefits.'"[1] The Connecticut Supreme Court majority in *O'Reggio* adopted this construction, noting that doing so was consistent with the court's long-standing principle and the legislature's intent that CFEPA "be interpreted in accordance with" its federal counterpart, Title VII of the Civil Rights Act of 1964.

The dissenting opinion, however, took the position that Connecticut non-discrimination statutes provide greater protections than their federal counterparts and that "a more expansive definition "of supervisor should therefore be applied when enforcing those statutes. The dissenters said they would hold employers responsible for the actions of any employee who has authority "to direct the day-to-day responsibilities of subordinates."

It is worth noting that before *O'Reggio*, the Connecticut Supreme Court had not expressly ruled that the *Faragher/Ellerth* affirmative defense applies to claims brought under CFEPA. In reaching its decision on the proper

definition of supervisor, the court seems to have assumed, although without saying so, that the *Faragher/Ellerth* defense would indeed apply to state law claims.[2]

Why Is This Important?

The *O'Reggio* decision resolves legal ambiguity by formally adopting a definition of "supervisor" for purposes of liability under CFEPA. This does not mean that employers can simply insulate themselves from such liability by purporting to restrict decision-making authority to a very small group. An employer could still be held vicariously liable for the actions of an employee who was not called a supervisor but who was effectively empowered to hire, fire or discipline through delegation of authority.

To help clarify roles, employers should make clear who has authority to take tangible employment actions and what responsibilities may or may not be delegated. They should also have clear policies against discrimination, harassment and retaliation, procedures for receiving complaints and responsive approaches to investigating such complaints. Even if the alleged harasser is not a supervisor, an employer may still be found liable for harassment if the plaintiff shows that the employer knew of the harassment and failed to take prompt and effective remedial action.

CLICK HERE FOR SOURCE ARTICLE

Personal Does Not Mean Private: Ninth Circuit Holds Personal Social Media Posts Can Constitute Workplace Harassment

Seyfarth Synopsis: *The Ninth Circuit has held that harassing conduct that takes place outside of the physical workplace can constitute workplace harassment*.

In the case of *Okonowsky v. Garland*, 23-55404.pdf (law360news.com), the Ninth Circuit considered a claim that social media posts made by a co-worker on a personal account constitute actionable workplace harassment under Title VII. The appeals court firmly "reject[ed] the notion that only conduct that occurs inside the physical workplace can be actionable, especially in light of the ubiquity of social media and the ready use of it to harass and bully both inside and outside of the physical workplace."

Lindsay Okonowsky was employed as a psychologist by the federal Bureau of Prisons at a correctional facility in Lompoc, California. As the Special Housing Unit ("SHU") psychologist, Okonowsky worked with custody staff to determine where inmates would be housed within the SHU so as to avoid conflict and violence among the inmates in the Unit. Okonowsky also relied on SHU custody officers to transport inmates from their cells to their clinical appointments with her and protect her in those interactions with inmates.

Steven Hellman, a corrections Lieutenant at the SHU at Lompoc, supervised custody staff in the SHU. Hellman and Okonowsky's jobs occasionally required them to collaborate or, at a minimum, to work side-by-side in the SHU. Around January 2020, Hellman and Okonowsky had apparent disagreements over how to manage "difficult inmates" in the SHU, and Hellman also became frustrated with Okonowsky.

During this time, Hellman created a social media account called "8_and_hitthe_gate." The page was followed by more than one hundred Lompoc employees, including the Human Resources Manager, the Union President, and a member of the prison's Special Investigative Services. Approximately half or more of the followers of the page were Lompoc employees. Okonowsky eventually discovered the account and saw posts that referred to the psychology department or "the psychologist" at SHU, including some posts that containing derogatory images resembling her likeness. Okonowsky understood these posts to refer to her specifically.

Some of the posts Okonowsky saw on Hellman's account displayed or suggested violence against and/or sexual contacts with women co-workers or violence against women generally. These posts were graphic, suggestive of rape and physical harassment, and depicted scenes of violence against women in general, but also against "the SHU psychologist" in particular. The Ninth Circuit specifically noted that "[m]ost of the posts are too graphic and disturbing to republish here," but recounted one in which Hellman joked that his subordinates – all male custody officers — would "gang bang" Okonowsky at her home during an end-of-the-quarter celebration she had scheduled at her home (before discovering the "8_and_hitthe_gate"

account). Okonowsky cancelled the gathering once she saw this post.

Okonowsky made a number of complaints about the posts on the "8_and_hitthe_gate" account over a period of months. Frustrated over what she perceived as a lack of response and concern for her safety by the Bureau of Prisons, Okonowsky transferred to a facility in Texas. She subsequently filed suit against the Bureau, asserting a single claim of sex discrimination under Title VII of the Civil Rights Act of 1964.

A federal district court judge in California granted summary judgment to the Bureau. The district court concluded that judgment should be entered in the Bureau's favor because the posts before it "occurred entirely outside of the workplace" on a staff member's personal social media account and were never sent directly to Okonowsky, displayed in the workplace, shown to Okonowsky in the workplace, or discussed with Okonowsky in the workplace without her consent. Therefore, the district court concluded that there was no triable issue of fact that Hellman's social media posts constituted severe and pervasive workplace harassment.

Okonowsky appealed. On appeal, since the parties did not dispute the first two elements of an actionable claim for a sexually hostile work environment (i.e., that Okonowsky was subjected to verbal or physical conduct of a sexual nature and that it was unwelcome), the Ninth Circuit focused its attention on the third element: whether or not Okonowsky had "adduced evidence of sufficiently severe or pervasive sexually offensive conduct from which a reasonable juror could conclude that Okonowsky's work environment was objectively hostile from the perspective of a reasonable juror." In doing so, the Ninth Circuit looked to "the totality of the circumstances" surrounding Okonowsky's claim.

The government contended before the appeals court that Okonowsky had failed to establish an objectively hostile work environment because the social media posts considered by the district court "occurred entirely outside of the workplace." The Ninth Circuit rejected the government's position as "grounded on legally and factually erroneous assumptions." The appeals court held that, given "[s]ocial media posts are permanently and infinitely viewable and re-viewable by any person with access to the page or site on which the posts appear. . . it makes little sense to describe a social media page that includes overt comments about a specific workplace, like Hellman's, as 'occuring' in only a discrete location." In other words, social media posts cannot be viewed as occurring strictly outside of the workplace because they can be seen at any time from any place, including from the workplace. The appeals court emphasized that the "crucial inquiry" was not "whether Hellman posted from work or his co-workers interacted with his page while at work, but whether his and his co-workers' discriminatory conduct had an unreasonable effect on Okonowsky's work environment."

Applying this standard, the Ninth Circuit concluded that "offsite and third-party conduct can have the effect of altering the working environment in an objectively severe or pervasive way" because "even if discriminatory or intimidating conduct occurs wholly offsite, it remains relevant to the extent it affects the employee's working environment," which in this case it clear did.

The Ninth Circuit's holding is an additional piece of the complex compliance puzzle facing employers when it comes to addressing the impact of personal social media posts in the workplace. The holding in *Okonowsky* makes crystal clear that employers cannot risk sticking their heads in the sand when employees complain about bullying or harassing posts they have seen on co-workers' personal social media accounts. However, in addition to the responsibility employers have to promptly and effectively address workplace harassment and take corrective action, they have some significant legal restrictions to keep in mind as they act in these situations.

First, a handful of states have laws that prohibit employers from taking action against employees for engaging in lawful off-duty conduct. A post might be offensive and violate a workplace anti-harassment policy, but might not be illegal. Second, there is the issue of obtaining access to the personal social media account at issue in connection with an investigation. More than half of the states in the U.S. have social media privacy laws that restrict an employer's access to non-public posts on personal employee social media accounts. However, most of these laws have exceptions that allow for employee access in the event of an investigation into workplace misconduct. The Ninth Circuit's holding in *Okonowsky* provides grounds for an employer to take the position that postings on a personal social media account can constitute workplace harassment and therefore violate an employer policy against harassment. (Whether or not this interpretation of the term "workplace misconduct" as used in state social media privacy laws will be carry the day remains to be seen.) Third, employers must also comply with state and federal laws concerning access to stored electronic communications when looking at employee social media posts. The federal Stored Communications Act and state law equivalents place restrictions on an employer's

ability to access communications in electronic storage, like social media posts.

In light of the holding in *Okonowsky*, employers should ensure that their anti-harassment policies make clear that they will not tolerate harassing, threatening, and derogatory social media interactions between co-workers even if they take place on personal social media accounts. Employers should also ensure that any anti-harassment training they conduct covers this issue and provide supervisors with the tools they need to respond appropriately to concerns raised about social media posts by employees. With employees connecting and communicating online "outside" of the workplace through myriad social media platforms and group messaging apps, employers must be ready to address harassment that seeps into the workplace through these channels. The Ninth Circuit's holding in *Okonowsky* makes it clear that employers who fail to address alleged harassment through personal social media postings do so at their own peril.

CLICK HERE FOR SOURCE ARTICLE

INTERNATIONAL DEVELOPMENTS

Philippines Tries Again to Pass Bill on Medical Cannabis Use

The Philippines is trying again to pass a bill allowing the use of cannabis for medical purposes after past failed attempts, with the House of Representatives approving a measure on Tuesday.

The approved House bill proposes to create a medical cannabis office under the Department of Health that will formulate rules on its use. A similar measure is under debate in the Senate, but it has faced opposition from lawmakers including the president's sister Imee Marcos. The bill needs to clear the Senate before it is submitted for approval to President Ferdinand Marcos Jr.

If passed into law, the move will make the Philippines one of the few countries in Asia to legalize use of medical cannabis, including South Korea. Thailand is discussing plans to regulate its own cannabis industry amid its leadership's push to outlaw it again to clamp down on rampant recreational use.

During his campaign in 2022, Marcos said he's in favor of legalizing medical cannabis as long as it has strict regulations, but he hasn't commented on Congress' recent moves to enact it. His predecessor, Rodrigo Duterte, opposed the move even after it was approved by the House of Representatives during his administration.

The Philippines currently classifies cannabis as a dangerous drug, and its use, cultivation and possession are punishable under its laws.

CLICK HERE FOR SOURCE ARTICLE

Tenant Background Checks in Canada: Balancing Screening and Privacy

The Privacy Commissioner of Canada (the "**Federal Commissioner**"), the Information and Privacy Commissioner for British Columbia (the "**B.C. Commissioner**") and the Information and Privacy Commissioner of Alberta (the "**Alberta Commissioner**") recently announced a joint investigation into the privacy compliance of Certn, a Canadian company that offers tenant screening services across Canada.[1] In particular, the commissioners stated that they will investigate whether Certn ensures that the information it collects, uses, and discloses for the purposes of tenant screening is sufficiently accurate, complete, and up to date, and whether the purposes for which it collects that information are appropriate. This announcement follows the B.C. Commissioner's 2018 investigation report on tenant screening and algorithms.[2]

The announcement signals to landlords and property managers across Canada that privacy regulators are looking closely at privacy compliance in the real estate industry. The Federal Commissioner cautions that "[l]andlords, and the services that they employ, must comply with Canadian privacy laws." Accordingly, landlords and property managers should take steps to ensure that their tenant screening practices comply with all applicable privacy laws. In this blog post, we describe some of the main privacy laws that may apply to different types of tenant screening, including social media checks and criminal background checks.

1. **Privacy Law**

Privacy laws vary across Canada. In British Columbia and Alberta, the province's respective *Personal Information Protection Act* ("**PIPA**") generally applies to the collection, use, and disclosure of personal information by private sector organizations.[3] In many other Canadian provinces, including Ontario, the federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") generally applies to private sector organizations.[4]

Key principles reflected in PIPEDA and the PIPAs include:

- **Consent:** Organizations must obtain informed consent before collecting, using, or disclosing someone's personal information or rely on one of the narrow exceptions to the consent requirement.[5] Depending on the circumstances, consent may be express or implied.

- **Limits:** Organizations may generally collect, use, and disclose personal information only to the extent necessary for the relevant purposes, and only if a reasonable person would consider the collection, use, or disclosure appropriate in the circumstances.
- **Accuracy:** Organizations should generally ensure that the personal information they collect, use, and disclose is accurate, complete, and up to date as necessary, taking into account the relevant purposes and the interests of the individual.

With these principles in mind, we describe below common types of tenant screening checks and some of the privacy considerations they may raise.

2. **Social Media Checks**

The B.C. Commissioner has cautioned that internet searches for information about prospective tenants are almost never authorized under B.C. privacy law.[6] Similarly, the Alberta Commissioner "generally discourage[s]" such searches given the privacy issues that may arise through an inadvertent collection of personal information.[7]

In B.C., it is a common misconception that landlords and property managers may review a prospective tenant's social media accounts without consent. Searching an applicant on the internet, including on social media, is generally considered a collection of personal information under B.C. privacy law. Although there are a few express allowances for collecting information on publicly available sources without consent, including professional business directories, newspapers, and magazines, these narrow exceptions do not include social media.[8]

The B.C. Commissioner has warned that even if an organization obtains consent, collecting this information remains risky because: (i) there is a tendency to collect more information than a reasonable person would consider appropriate in the circumstances; (ii) it is often difficult to confirm the accuracy of information that is viewed and collected online; and (iii) social media searches may inadvertently disclose information about third parties who did not consent to the search.[9] Accordingly, even with consent, viewing personal information about a prospective tenant on search engines and social media platforms may not meet PIPA's reasonableness requirement.

PIPA's accuracy requirements also present challenges for this form of background check.[10] Organizations must make a reasonable effort to ensure that the personal information it collects is accurate and complete if that information is likely to be used to make a decision that affects the individual, or if it is likely to be disclosed to another organization. Determining and verifying the accuracy of information collected via social media can be challenging if not impossible.

A further level of complexity is that organizations would need to take screenshots of every page viewed. Where an organization in B.C. uses personal information about an individual to make a decision about them, the organization must retain the information for at least one year and provide a copy to the individual on request (subject to some narrow exceptions).[11]

3. **Criminal Record Checks**

The B.C. Commissioner has stated that in most situations, running a criminal record check on a prospective tenant will be neither necessary nor reasonable.[12]

Former B.C. Commissioner Elizabeth Denham pointed out in her 2014 report on the *Use of Police Information Checks in British Columbia* that little research has been conducted on the usefulness of criminal record checks.[13] Also, these checks can reveal sensitive personal information about a person's past activities, including mental health information, prior convictions, penalties and outstanding charges, and details about contact with police. This information may be untested, unproven and stigmatizing.

Landlords and property managers in British Columbia cannot require a prospective tenant to consent to a criminal record check as a condition of providing a rental unit, unless the information is necessary. In some situations, landlords and property managers may be able to justify running these checks, such as if there is a daycare in the rental building.[14] In all cases, landlords and property managers should have clear reasons for why they need the information.

4. **Checks involving information protected under human rights laws**

In British Columbia, landlords and property managers cannot refuse to rent to someone based on their race, colour, ancestry, place of origin, religion, marital status, family status, physical or mental disability, sex, gender identity or expression, age, sexual orientation, or lawful source of income.[15] There are limited exceptions to this rule, including that landlords and property managers can refuse to rent a residence to individuals under 55 if the unit is a residential complex where every unit is reserved for someone over 55.[16]

The B.C. Commissioner has noted that using information protected under the *Human Rights Code* is generally not a purpose that would be appropriate, so landlords and property managers are generally not authorized to collect this information.[17]

5. **Public Records Checks**

In British Columbia, landlords and property managers can collect information from a narrow set of prescribed publicly available sources without consent. These sources include: (i) registries that the public has a right to access, such as court registries and records of residential tenancy disputes; and (ii) printed or electronic publications, such as magazines, books, and newspapers.[18] Although landlords and property managers do not require consent to collect information from these sources, they must notify a prospective tenant beforehand if they intend to use the tenant's name to collect information from these sources.[19]

6. **Employment/Income Verification**

It may be reasonable for landlords and property managers to conduct searches to collect information about a prospective tenant's proof of income or employment if they cannot verify the tenant's employment through references.[20] As with other types of searches, landlords and property managers should obtain tenants' consent before running these searches.

7. **Credit Reports and Histories**

Credit reports contain personal, financial, and credit history information that can be used to make decisions about tenancies, employment, and other applications that consider financial responsibility as a factor. In most provinces, individuals must consent for a business or individual to use their credit report. In Nova Scotia, Prince Edward Island, and Saskatchewan, individuals need only be informed that their credit report is being checked. In his 2018 report, the B.C. Commissioner recommended that:

- "Landlords should only require a prospective tenant to consent to a credit check, and provide information to allow the landlord to perform a credit check, when the prospective tenant cannot provide sufficient references about previous tenancies or satisfactory employment and income verification"; and
- "Landlords should explicitly state whether the credit report they collect could lower the prospective tenant's credit score. They must also state on the form which credit reporting agencies are providing the information."

In British Columbia, the *Business Practices and Consumer Protection Act* requires organizations to have evidence that the individual consented to such a report. This is usually done by including a consent in an application for credit, insurance, employment, or tenancy.[21]

Tenant Screening Services

Landlords and property managers have an interest in selecting tenants that are reliable and responsible. But before accessing a screening service that involves the collection, use, or disclosure of personal information about prospective tenants, landlords and property managers should consider their obligations under all applicable privacy laws. They cannot rely on third parties to collect and use personal information on their behalf that they themselves would not be authorized to collect or use.[22] Accordingly, they should be aware of their obligations under applicable privacy laws and assess service providers' compliance when considering outsourcing tenant screening.

The investigation into Certn will likely provide additional insights on the application and interpretation of privacy laws in the context of tenant screening. If you have any questions about tenant screening or privacy law more generally, please contact our Cyber/Data team.

CLICK HERE FOR SOURCE ARTICLE

The Data Protection Legal Framework in Canada

Law and the regulatory authority

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

In Canada, privacy laws are overseen by privacy commissioners at the federal, provincial and territorial levels and enforced through various government organisations and agencies (collectively 'privacy regulators'), including:

- Federal: The Office of the Privacy Commissioner of Canada (OPC);
- Alberta: The Information and Privacy Commissioner of Alberta (Alberta OIPC);
- British Columbia: The Information and Privacy Commissioner for British Columbia (BC OIPC); and
- Quebec: Quebec Information Access Commission (Quebec CAI).

The OPC is responsible for conducting investigations in response to complaints by individuals regarding the mishandling of their PI by organisations. The Alberta OIPC, BC OIPC, and Quebec CAI have similar investigative powers for complaints arising from within their provinces.

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Data protection authorities in Canada are not obligated to cooperate with data protection authorities from within or outside Canada; however, there are a number of discretionary legal instruments that enable them to do so, as follows.

- The OPC reserves the power to consult with provincial privacy regulators in Canada to coordinate the activities of its office and to handle complaints of mutual interest. The OPC also has the power to cooperate with data protection authorities in foreign states. This power allows the OPC to share information that is relevant or could assist with an ongoing or potential investigation or complaint.
- Privacy regulators in Canada may use a Memoranda of Understanding with foreign data protection authorities, which does not mandate but encourages cooperation based on a common understanding.

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Yes, federal and provincial privacy laws provide administrative sanctions and criminal consequences for non-compliance with and breaches of privacy laws.

PIPEDA provides that it is an offence to knowingly infringe statutory and regulatory breach reporting and notification obligations, which generally require a person or business to report an incident to the OPC involving unauthorised access to or disclosure or PI that has the potential to create a 'real risk of significant harm' (RROSH) to one or more data subjects impacted by the incident, and to notify individuals that may have been impacted by such an incident as soon as is feasible. Failure to report an RROSH incident or to notify affected individuals can result in an indictable offence and gives the OPC power to impose a fine not exceeding C$100,000.

Under the Alberta PIPA, the Alberta OIC can impose a fine not exceeding C$100,000 for failure to report a prescribed privacy incident or to notify affected individuals. Under the Quebec Act, the Quebec CAI can impose a fine not exceeding C$25,000,000 or 4 per cent of the business' worldwide turnover for the preceding fiscal year for failure to report a prescribed confidentiality incident or notify affected individuals.

Scope

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Privacy laws in Canada do not cover all sectors; the specific scope of a privacy law depends on the law itself and whether it falls under federal or provincial jurisdiction. For example, the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to an organisation that collects, uses or discloses PI in the course of commercial activities (eg, not-for-profit or charitable activities could be excluded) or where such activities relate to an employee or applicant for employment in connection with the operation of a federal work, undertaking or business. PIPEDA may not apply to the collection, use or disclosure of PI from employees in a non-federally regulated sector.

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

There are federal and provincial laws that govern the interception of communications and the electronic monitoring and surveillance of individuals. With respect to interception, Canada's Criminal Code makes it an indictable offence, punishable by up to five years in prison, to knowingly intercept a private communication by means of any electro-magnetic, acoustic, mechanical or other device; however, the Code recognises that interception may be permissible with the originator's consent. The Criminal Code also gives law enforcement the power to access private communications in certain circumstances, generally where they have obtained a valid warrant or judicial authorisation.

Ontario's Employment Standards Act 2000 requires employers with 25 or more employees in the province to have a written electronic monitoring policy that informs employees about the means of electronic monitoring and purposes for such monitoring.

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

Canada's Anti-Spam Law imposes obligations on persons and businesses that send commercial electronic messages (CEMs), which are electronic messages, in any form, that are sent for a commercial purpose (eg, marketing emails or messages sent to a person's social media inbox). Generally, a business is required to obtain an individual's express consent before sending them a CEM, unless a limited exception applies that would allow the business to rely on implied consent (eg, in circumstances where the recipient of the CEM is a prior or existing customer). CEMs must also contain an unsubscribe mechanism.

The Office of the Privacy Commissioner of Canada (OPC) has also published guidance on online behavioural advertising and the use of cookies, which sets out the conditions under which implied consent to online behavioural advertising can be considered acceptable. The guidance also generally prohibits the use of certain types of cookies and generally prohibits the tracking of children and tracking on websites aimed at children. In the context of behavioural advertising, data subjects must be given the ability to decline tracking technologies (eg, use of cookies).

PI formats

What categories and types of PI are covered by the law?

Federal and provincial privacy laws cover a wide range of PI, including any information, irrespective of format (eg, recorded, audio, video, or otherwise), which creates a serious possibility that, alone or combined with other information, a natural person could be personally identified.

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

PIPEDA can have extraterritorial effect where there is a sufficient nexus to Canada. While PIPEDA is silent on its territorial reach, the Federal Court held in *AT v Globe24h.com*, 2017 FC 114, that PIPEDA applies where there exists a 'real and substantial link' to Canada. In terms of whether such a link exists, determination will be made on a case-by-case basis, taking into account factors such as the location of the individuals, the organisation collecting the PI and the service provider processing the PI.

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

All processing of PI is covered, although the duties and responsibilities differ between those that control the PI and those that process the PI. Those that control the PI, which are generally the organisations that own the PI or for whom the PI was initially collected, are accountable for such PI under PIPEDA, Schedule 1 (Fair Information Principles). Included in the Fair Information Principles is the requirement to ensure through contractual means that the PI receives adequate protection if it is transferred to another entity, such as a service provider, for processing. Service providers or processors are therefore not held accountable directly through PIPEDA, but through contractual agreements with the organisation that controls the PI.

CLICK HERE FOR SOURCE ARTICLE

Finland - Breach of Data Protection Regulations by Publishing the Employees' Personal Phone Numbers on the Employer's Intranet

At a glance

- A company published on its intranet the personal phone numbers of 300 bus driver employees.
- The Deputy Data Protection Ombudsman considered that this practice violates data protection laws. He ordered the company to change its practice.

The Deputy Data Protection Ombudsman considered that a company had breached data protection rules by publishing on its intranet the personal phone numbers of 300 bus driver employees in a way that they were available to all bus drivers in the company. The publication of personal phone numbers constituted a disclosure of personal data to third parties, and there were no legal grounds for the disclosure. Communication between bus drivers can also be organised in a way that is less privacy-intrusive, such as via work telephone.

In principle, employees' personal telephone numbers or e-mail addresses should only be used if it is not possible to use a work telephone number or work e-mail address. In addition, employees' personal data should only be processed by persons whose tasks include the processing of such data, eg managers or persons working in personnel management.

In its decision of 20 June 2024, the Deputy Data Protection Ombudsman issued a warning to the company for breaching data protection laws and ordered the company to change its practice.

CLICK HERE FOR SOURCE ARTICLE

Saudi Arabia's Personal Data Protection Law and its implications for data controllers

As the grace period for compliance with the Saudi data protection law is rapidly drawing to a close, the Saudi Data and AI Authority ("SDAIA") *has published draft rules on the operation of the national register of controllers.*

Data controllers subject to the Saudi Personal Data Protection Law ("PDPL") are currently protected by an implementation grace period, but enforcement of the PDPL is due to commence in September this year, meaning the grace period will shortly end and controllers have little time left to complete compliance readiness. Given that the draft rules have only recently been published for consultation, it is possible that enforcement of certain aspects of the Law, such as the obligation to register as a controller (if applicable – please see below), may be phased in.

The rules define the national register as a "a way to monitor and follow up on Controllers, as well as assist them in raising their level of compliance with the Law and the Regulations. Additionally, the National Register provides services related to personal data protection procedures."

Registration not mandatory for all

The most significant section of the rules is Article 2 which provides that only the following controllers (if located within KSA) will mandatorily need to register:

- Public entities;
- Controllers whose main activity is based on personal data processing and collection; and
- Controllers who collect and process sensitive personal data, and the processing is likely to entail a high risk to the rights and freedoms of the personal data subjects.

Although registration will therefore not be mandatory for all controllers, subject to any further guidance as to the interpretation of the criteria, we consider that the obligation is likely to impact many enterprises.

Non-Saudi controllers

It is worth emphasising that the PDPL applies not just to Saudi entities, but to any entity which processes the personal data of people resident in KSA. This approach, taken literally, presents potential difficulties to businesses which do not actively target the KSA market but which may process some KSA-resident data on a passive or unsolicited basis. Helpfully, the introduction to the draft rules specify that separate registration rules will be published for controllers located outside KSA. It will be interesting to see if any additional nuances are also introduced to confirm the scope of the law to non-Saudi businesses.

Registration process

The Rules detail the registration procedures, which will vary based on the type of entity.

- Public entities must complete the registration form provided by SDAIA and appoint a delegate to handle the process, which includes assessing the need for a Personal Data Protection Officer.
- Private entities shall initiate registration on the Platform, through an owner, partner or delegate, and the process involves filling out necessary fields, verifying eligibility and assessing the need to appoint a Data Protection Officer.
- Individuals can register by completing the required procedures, including filling out the registration form and verifying eligibility.

We assume that the "delegate" referred to in the rules may be an employee of the controller, although some clarification around this point would be welcomed in the final version.

Certification

The rules also imply that the controller will be able to generate its own registration certificate as part of the registration process, which will include a QR code for verification. SDAIA will notify the controller when the registration is due for renewal at least thirty days before the expiry date. It is not clear at this stage how long a registration will be valid for before

it expires.

To enhance public trust in the services provided, SDAIA will implement mechanisms for public verification of controllers' registrations, making registration certificates accessible within a National Register for Personal Data Protection.
Summary

With the PDPL due to start being enforced in a matter of weeks, the new draft rules represent welcome and pragmatic guidance on one aspect of the law. However, it is important for all Saudi controllers and processors to understand that the administrative requirements of the law are a small part of overall compliance, and it is important to ensure that a holistic privacy framework and culture of data protection is developed.

CLICK HERE FOR SOURCE ARTICLE

MISCELLANEOUS DEVELOPMENTS

When Social Media Posts Become Workplace Harassment

Highlights

- The U.S. Court of Appeals for the Ninth Circuit recently ruled that companies can be held liable for hostile work environment claims under Title VII of the Civil Rights Act of 1964 if an employee shares harassing content online on their personal social media that negatively impacts the workplace.
- This is the first appeals court decision on employee use of social media outside of the workplace since the Equal Employment Opportunity Commission (EEOC) issued updated guidance on sexual harassment on April 29, 2024.
- The updated EEOC guidance specially addresses how employee use of social media outside of the workplace can create or contribute to a sexually hostile work environment.

The U.S. Court of Appeals for the Ninth Circuit on July 25, 2024, ruled that under Title VII of the Civil Rights Act of 1964, companies can be held liable for claims of a hostile work environment if an employee shares harassing content online that negatively impacts the workplace.

Case Summary

In *Okonowsky v. Merrick Garland*, the Ninth Circuit overturned a trial court's decision on summary judgment in favor of the government in a sexual harassment case brought under Title VII of the Civil Rights Act of 1964.

The case was brought by a staff psychologist working at a federal prison where she claims that her employer, the Federal Bureau of Prisons, failed to address a sexually hostile work environment created by her co-worker. The psychologist claimed that a co-worker posted derogatory content on social media. Despite reporting this to her employer, the co-worker continued to post even after being directed to stop in accordance with the prison's anti-harassment policy. The psychologist eventually resigned due to the lack of action and filed the lawsuit.

The trial court granted summary judgment to the prison, ruling that the social media posts were "entirely outside of the workplace" because they were made on a personal account and not shared or discussed with plaintiff in the workplace. The court found that since the posts did not constitute severe or frequent harassment within the physical workplace, there was no triable issue regarding whether the plaintiff's work environment was objectively hostile.

The Ninth Circuit disagreed with the trial court and found that online social media contact can constitute workplace harassment. The court noted that it "rejected" the "notion that only conduct that occurs inside the physical workplace can be actionable, especially in light of the ubiquity of social media and the ready use of it to harass and bully both inside and outside of the physical workplace." The court further warned that "Social media posts are permanently and infinitely viewable and re-viewable by any person with access to the page or site on which the posts appear" and that "even if discriminatory or intimidating conduct occurs wholly offsite, it remains relevant to the extent it affects the employee's working environment." The Ninth Circuit sent the case back to the trial court.

The Ninth Circuit's decision is consistent with recent guidance from the U.S. Equal Employment Opportunity Commission (EEOC) on sexual harassment and the use of social media accounts by employees. It reads in part: "Although employers generally are not responsible for conduct that occurs in a non-work-related context, they may be liable when the conduct has consequences in the workplace and therefore contributes to a hostile work environment." The EEOC also noted that "[c]onduct that can affect the terms and conditions of employment, even if it does not occur in a work-related context, includes electronic communications using private phones, computers, or social media accounts, if it impacts the workplace."

Key Takeaways

- Companies should conduct thorough investigations into any employee claims of a hostile work environment (whether based on sex, race, origin or any other protected classification), including complaints about co-workers' social media posts. In addition, companies should train employees in managerial positions on how to handle such claims.

- Companies should consider updating their anti-harassment and social media policies to address strategies for preventing harassment and other problematic online behavior to reduce workplace issues.

CLICK HERE FOR SOURCE ARTICLE

Marijuana Legalization Leads U.S. Workers to Increasingly Test Positive and Cheat on Employer Drug Screens

According to Quest Diagnostics, one of the nation's leading drug-testing laboratories, positive marijuana tests among the U.S. workforce increased to 4.5% in 2023. The percentage of positive tests was 4.3% in 2022 and 3.1% in 2019. In 2023, Quest conducted about 8.4 million urine drug tests for employers, plus 1.3 million oral fluid tests and 73,000 hair tests. Meanwhile, the overall percentage of workers testing positive for any illegal drugs has held steady at 4.6% for the past three years, significantly down from 13.6% in 1988, when workplace drug-testing programs started.

Quest also found an increase in workers cheating on drug tests, which often occurs when workers replace their urine with someone else's urine or synthetic samples bought online. Another common drug-testing cheating method is when workers submit invalid specimens, which suggests that they have been mixed with an additive. Quest stated that out of 5.5 million urine samples collected from workers last year, about 6,000 were classified as substituted, and 25,000 were classified as invalid. The number of invalid tests increased by 45% from the prior rate, reaching an all-time high.

The increase in positive marijuana tests is not surprising, given that society is becoming more accepting of its use, and many states have legalized it, either medically, recreationally, or both. As more people use marijuana, test results inevitably will rise. Predictably, those states that have legalized recreational marijuana have seen the greatest increases in positive marijuana tests for workers.

Currently, two dozen states and Washington, D.C., allow recreational marijuana use. Still, marijuana remains classified under federal law as a Schedule I drug, although the Biden administration is seeking to downgrade it to a less serious Schedule III drug.

Quest's statistics also showed a significant increase in 2023 positive marijuana tests among white-collar workers in 13 of 15 industries. Positive tests in finance and insurance increased by over 35%, while tests in public administration rose almost 24% and real estate by 22%. While it is unclear what has caused the spike in marijuana usage among white-collar workers, it may be the product of unprecedented stress and isolation during the pandemic and work-from-home policies that have continued after the pandemic.

In response, some employers are rethinking their drug-testing policies to take differing state laws into account, and some are moving away from testing for marijuana altogether. Still, other employers are drug-testing workers only if they suspect impairment at work or during random and pre-employment tests.

Reclassifying marijuana as a Schedule III drug still would leave a conflict between federal law and many state laws. A Schedule III classification could mean that marijuana would be available with a prescription under federal law.

CLICK HERE FOR SOURCE ARTICLE

How to Conduct a Workplace Investigation

Investigations of employee discrimination and harassment complaints are necessary to provide factual basis for decision-making.

Employee complaints of discrimination and harassment must always be taken extremely seriously.
Investigations of complaints are necessary to provide a factual basis for the employer's decision-making and to mitigate potential risks. A proper investigation allows a company to determine what happened, deal with employee problems early on, appropriately enforce company policies and rules, and mitigate liability. Multiple steps are needed to conduct a proper investigation. Employers should:

1. Respond promptly.
2. Ensure discrimination or harassment stops immediately.
3. Choose an investigator.
4. Gather and review background information.
5. Conduct interviews.
6. Document the investigation.
7. Make a decision.
8. Prepare the investigation report.
9. Use corrective action, as appropriate.
10. Close the investigation.

Best practices for conducting a proper investigation

An employer must make the investigation a top priority and promptly identify an investigator and a decision-maker who are free of real or perceived conflicts of interest or bias. A good investigator should possess the following abilities:

- Good listening skills.
- Capable of handling uncomfortable subjects and maintaining confidentiality.
- Detail oriented.
- Make findings in the face of conflicting evidence.
- Write a concise and coherent report.
- Presents well as a witness in any future litigation.

Human resources professionals often make great investigators. However, on a case-by-case basis, employers should consider utilizing in-house or outside counsel to conduct investigations in order to best navigate serious or complex complaints and to enhance the likelihood that certain related communications are and remain privileged.

During an investigation, the most common order of interviews is:

1. The complainant/victim.
2. Key witnesses.
3. The accused.
4. Other witnesses identified during the investigation.
5. Any follow-up interviews for witnesses to respond to or address statements of others.

This order best allows the investigator to gain sufficient knowledge in order to effectively interview the accused.

When interviewing the accused, the investigator should not offer a personal opinion. Instead, the interview should be designed to give the accused an opportunity to provide his or her version of the events as well as any additional information to be considered. If the accused refuses to participate, the investigator should advise him or her that the company will be forced to base its decision on the other information gathered during the investigation, the inferences drawn from the evidence, and the accused's unwillingness to cooperate with the interview.

In most non-union settings, the accused does not have the right to legal representation during the interview. However, in some circumstances, it may make sense to allow attendance of legal counsel, provided that they do not interfere with the investigation.

After completing interviews, the investigator prepares a written summary of findings and determinations. This summary should identify the persons interviewed, dates of interviews, and documents and other information reviewed. The investigator will likely have to weigh evidence and assess credibility to make their final determination(s). When making credibility determinations, the investigator should consider how each witness presented, whether the witness's version of events was corroborated or undisputed, and the potential motives of each witness.

Following the investigation, any remedial measures should be designed to ensure that no further discrimination or harassment occurs and correct the effects on the complainant, to the extent applicable. In addition, employers must take

preventative measures to ensure that the complainant is not retaliated against for making a good-faith complaint.

There are many pitfalls when conducting an employment investigation. Employers are well advised to consult with their employment attorneys before and while conducting an investigation in order to mitigate risks.

CLICK HERE FOR SOURCE ARTICLE