SEPTEMBER 2024

CLEARSTAR®

SCREENING COMPLIANCE UPDATE

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

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

CLICK FOR PAST UPDATES

CLEARSTAR®

TABLE OF CONTENTS

SCREENING COMPLIANCE UPDATE | SEPTEMBER 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

September 2024 Screening Compliance Update Executive Summary

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

- FEDERAL DEVELOPMENTS: Although the Drug Enforcement Administration (DEA) has issued proposed regulations that would downgrade marijuana to a Schedule III drug with some legitimate uses, marijuana is still an illegal drug under federal law. Employees in positions that are subject to federal drug laws should be handled in accordance with the applicable federal regulations.
- STATE DEVELOPMENTS: Missouri has opened an investigation into a background check data aggregator over a data breach that has allegedly exposed information in more than 2.9 billion records while Illinois, Maryland, Massachusetts, and Minnesota have passed salary transparency laws.
- INTERNATIONAL DEVELOPMENTS: All employers in the United Kingdom (UK) will have a mandatory duty to take reasonable steps to prevent sexual harassment of their employees in the course of their employment starting October 26, 2024. The Equality and Human Rights Commission (EHRC) has updated its existing guidance on sexual harassment about the scope of this new duty.

I hope you find this month's 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

Workplace drug/alcohol policies in a legal weed world: 10 easy steps

Marijuana is still an illegal drug under federal law, although the Drug Enforcement Administration has issued proposed regulations that would "downgrade" marijuana to a Schedule III drug (some legitimate uses). Employees in positions that are subject to federal drug laws should be handled in accordance with the applicable federal regulations.

Step One: Know your jurisdiction(s). The laws relating to use of drugs (and, to a lesser degree, alcohol) are changing constantly, especially where use of marijuana and cannabis are concerned. At this moment, 38 states have legalized the use of medical marijuana. Recreational marijuana is legal in 24 states.

The applicable laws will normally be the laws in the states where your employees work. If your company has facilities in most states, or if you have a large and geographically dispersed remote workforce, that means you will have to keep up with a lot.

And it's not just drug laws that vary from state to state. Many states also have their own disability rights laws. If an employee is legally using medical marijuana to treat a medical condition, then he or she may be protected from discrimination and may be entitled to reasonable accommodation under state law. (As I said last week and say again below, the Americans with Disabilities Act does not protect medical marijuana users because marijuana is currently illegal under federal law.)

Step Two: Determine whether any of your jobs are "safety-sensitive," and, if so, which ones. "Safety-sensitive" can include people who operate heavy or dangerous machinery, and also white-collar sales representatives who are required to drive as part of their jobs. There are plenty of other jobs where impairment could endanger the employee, the employee's co-workers, or the general public. On the other hand, full-time desk jobs (either at an office or at home), would usually not be considered safety-sensitive. I am oversimplifying greatly, but you get the idea.

Step Three: With safety-sensitive jobs, decide what you want to do in the way of drug/alcohol testing, and (if the employee is in a state where marijuana use is legal) what you want to do about marijuana. A good general recommendation if you have employees in a jurisdiction where recreational use is legal is to treat marijuana use the same way you would treat alcohol use. You would not take action against an employee for enjoying a few beers at home after a hard day at work, but you might justifiably take action against an employee who was three sheets to the wind when *reporting* for work. Ditto for pot.

But this sounds simpler than it is. Alcohol has generally accepted measures for determining whether someone is "under the influence." Alcohol is also out of the system a few hours after consumption. Marijuana is more complicated because it stays in the body a long time, meaning people can test positive when they are arguably no longer "impaired." Also, we don't yet have a generally accepted measure for determining marijuana impairment. Several states have driving under the influence laws that put the level of marijuana impairment at 2-5 nanograms of THC per milliliter of blood. You might be able to adopt a similar standard for your workplace.

Step Four: Decide how aggressive you want to be with employees in non-safety-sensitive jobs. Yes, you can have one set of substance abuse policies for employees in safety-sensitive jobs and another set for everybody else. If the employee is in a state where recreational marijuana use is legal and the position is not safety-sensitive, you shouldn't be testing for marijuana unless you have (1) reasonable suspicion (2) based on objective evidence (3) to believe that the employee is impaired on the job, and (4) that the impairment is related to marijuana use (same as you'd treat an employee who seems to be drunk on the job).

But marijuana and alcohol aside, you can continue testing all employees for other controlled substances post-offer, on a random basis, based on reasonable suspicion, post-accident, and post-rehabilitation, unless a federal law controls or a specific applicable state law says you can't. (See Step One, above.)

Step Five: Decide how you want to handle employees who test positive. Do you want to take a hard line and fire them the first time they're caught? In many states, you can do that – but not all. (See Step One again.) Or, do you prefer to allow

them to go through an Employee Assistance Program, at least after a first positive result? In my experience, most employers allow one shot at an EAP if the employee signs a Last Chance Agreement. If the employee ever tests positive again, that's usually it.

Step Six: Realize that alcohol is in a class by itself from an ADA standpoint. As I discussed last week, alcohol addiction, even with current use, is a "disability" within the meaning of the Americans with Disabilities Act, meaning that employers cannot discriminate against employees based on alcoholism and also have to make reasonable accommodations on a limited basis. (You don't have to accommodate drinking on the job unless you allow non-alcoholic employees to do it, but you generally do have to allow an employee who is an alcoholic to have time off for rehab and things like that.)

The ADA does not protect "current users of illegal drugs," even if they are currently addicted. However, drug addicts *who are no longer current users* are considered persons with disabilities. So they are protected from discrimination and should also be allowed time off as needed to continue their treatment.

Step Seven: If your employees are in a state where marijuana use is still illegal . . . You may still have state laws that apply to drug testing, and you'll want to comply with those. (See Step One.) Otherwise, you should be safe to ban, test for, and terminate for use of marijuana as well as other illegal drugs.

Step Eight: If your employees are spread among states where recreational marijuana is legal, where medical-only is legal, and where marijuana is illegal . . . Quit your job now while you still can. Just kidding. Here are your options: (1) Comply with the most pro-marijuana law that applies, which means you'd be treating all of your employees as if recreational use is legal. The benefit is that you have a single standard that applies to everybody. That could minimize employee perceptions of unfairness, and it also could make your life a lot simpler. The downside is that you can't be as strict with marijuana use as you legally have the right to be. (2) Apply the applicable law to each employee, which means you'd be most lenient with the employees in recreational states, medium-lenient with the employees in medical-only states, and relatively strict with the employees in "illegal" states. The benefit of this is that you are not tolerating more use of marijuana than you absolutely have to. The downsides, of course, are perceptions of unequal treatment among your employees, and administrative headaches for you.

Step Nine: Don't forget about legal medications. You may have an applicant or employee who tests positive or is impaired on the job because of legal use of prescription medications, legal use of medical marijuana, or legal use of over-the-counter medications. If that's the case, the individual may be legally protected and may be entitled to reasonable accommodation. (Have I mentioned in the last five minutes that medical marijuana is still an illegal drug under federal law, so an employee using medical marijuana won't be protected by the ADA but may be protected by a state disability rights law? I feel like I have. See Step One.)

To use an example that involves neither marijuana nor alcohol, let's say Melvin, a welder with degenerative disc disease, is taking prescription opiates for the pain. Melvin in all likelihood has a "disability" within the meaning of the ADA based on his degenerative disc disease. Assuming welding is a safety-sensitive position (I'm gonna say it is, since it involves fire and molten metal), and that the opiates impair him enough to create a safety risk, then the employer may need to remove Melvin from his regular job duties, at least temporarily. This could include temporarily transferring Melvin to a non-safety-sensitive position or, if that isn't possible, allowing him to take medical leave until he is no longer on the medication or until his dose becomes low enough to be non-impairing.

In substance abuse policies, I normally include a provision that requires employees to notify Human Resources or another appropriate person in the company if they are taking any legal medications that could create a safety issue or impair the employee's ability to competently perform the duties of the job. But I also state in the policy that the employee will not be disciplined or discharged for making such a disclosure. Instead, the company will engage in the "interactive process" with the employee and (we hope) reach agreement on reasonable accommodations that will eliminate the risk or reduce it to an acceptable level.

Step Ten: Yes, this has all become ridiculously complicated. If this post hasn't convinced you, I don't know what will. Be sure to consult with qualified employment counsel when determining the laws that apply to your employees, deciding what you're going to do, and drafting and enforcing your substance abuse policies.

CLICK HERE FOR SOURCE ARTICLE

Swiss-U.S. Data Privacy Framework Principles

The Swiss-U.S. Data Privacy Framework is the latest development in a series of initiatives aimed at facilitating secure data transfers between Switzerland and the United States while protecting individuals' privacy rights. This framework follows in the footsteps of earlier agreements, such as the Safe Harbor Framework established in 2000, which allowed companies to transfer personal data from Switzerland to the U.S. under a set of agreed privacy principles. However, the Safe Harbor Framework was invalidated by the European Court of Justice in 2015 due to concerns about inadequate data protection, leading to the introduction of the EU-U.S. Privacy Shield in 2016, and subsequently, the Swiss-U.S. Privacy Shield, which aimed to address these issues by strengthening obligations on U.S. companies receiving personal data and offering more robust rights to individuals.

Despite these enhancements, the Privacy Shield frameworks were also invalidated in 2020 due to concerns that U.S. surveillance laws did not provide sufficient protections for data privacy. In response, the Swiss-U.S. Data Privacy Framework has been introduced as a more robust mechanism that seeks to address these legal challenges by incorporating stricter data protection principles, enhanced oversight, and stronger enforcement measures. This new framework aims to ensure that personal data transferred from Switzerland to the U.S. enjoys an equivalent level of protection to that within Switzerland, thereby facilitating continued transatlantic data flows while safeguarding individuals' privacy rights.

Swiss-U.S. Data Privacy Framework in the Context of FADP
The Swiss-U.S. Data Privacy Framework is designed to facilitate the secure transfer of personal data from Switzerland to the United States while ensuring compliance with Swiss data protection standards as outlined in the FADP.
The framework seeks to provide a level of protection for personal data that is equivalent to Swiss standards, aligning with Article 16's requirement that data can only be transferred abroad if there is adequate protection in place. The framework includes strict data handling requirements, oversight mechanisms, and enforcement measures that aim to match Swiss expectations, thereby allowing transfers without the need for additional safeguards like specific contracts or other guarantees.

In essence, the Swiss-U.S. Data Privacy Framework seeks to streamline cross-border data transfers between Switzerland and the U.S. by adhering to the principles of Article 16, providing a reliable mechanism for data protection that negates the need for additional contractual safeguards in most cases. At the same time, the exceptions in Article 17 ensure that necessary transfers can proceed even when standard protections are not fully in place, as long as specific conditions are met. This framework ultimately aims to harmonize U.S. data handling practices with Swiss legal requirements, supporting continued transatlantic data flows while safeguarding individual privacy rights.

Key Principles of the Swiss-U.S. Data Privacy Framework
The Swiss-U.S. Data Privacy Framework introduces several key principles designed to enhance the protection of personal data transferred to the United States. The framework is intended to provide U.S. organizations with a reliable mechanism for receiving personal data from Switzerland while ensuring that individuals' data privacy rights are protected. Here are some of the primary elements:

1. Self-Certification and Compliance
In order to participate in the Swiss-U.S. Data Privacy Framework, U.S. organizations must self-certify annually to the U.S. Department of Commerce. This self-certification confirms that they adhere to the framework's principles, which are designed to protect personal data transferred from Switzerland to the United States. The self-certification process includes:

- **Public Commitment**: Organizations must publicly declare their commitment to comply with the Swiss-U.S. DPF principles. This public declaration is binding and enforceable under U.S. law.
- **Regulatory Oversight**: Organizations must be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC), the Department of Transportation (DOT), or other statutory bodies that ensure compliance. This regulatory oversight provides a mechanism for addressing non-compliance, including potential penalties or sanctions.
- T**ransparency in Privacy Policies**: Organizations are required to disclose their privacy policies publicly, ensuring that these policies are in line with the Swiss-U.S. DPF principles. This transparency helps build trust with individuals whose data are being transferred.

A list of all certified companies is available here: Data Privacy Framework List

2. Data Handling Requirements
The Swiss-U.S. DPF sets strict guidelines on how organizations must handle personal data to ensure privacy and data security:

- **Notice**: Organizations must inform individuals about their participation in the framework, the types of personal data they collect, the purposes of data collection, and how individuals can contact the organization with inquiries or complaints. This notice must be clear, conspicuous, and provided when individuals first provide personal data or as soon as practicable thereafter.
- **Choice**: Organizations must offer individuals the choice to opt-out of their personal data being disclosed to third parties or used for purposes that are materially different from the original purpose of collection. For sensitive information, affirmative express consent (opt-in) is required.
- **Data Integrity and Purpose Limitation**: Personal data must be limited to what is relevant for the purposes of processing, and organizations must take reasonable steps to ensure that data is accurate, complete, and current. Data should only be retained as long as necessary for its intended purpose.
- **Security**: Organizations must implement reasonable and appropriate security measures to protect personal data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. These measures should take into account the risks involved in the data processing activities and the nature of the personal data.

3. Accountability for Onward Transfers
When personal data is transferred to third parties (e.g., service providers, subcontractors), the organization must ensure that these third parties adhere to the same level of protection as required by the Swiss-U.S. DPF principles:

- **Contractual Obligations**: The transferring organization must enter into a contract with third parties that stipulates that the data will be processed only for limited and specified purposes, and that the third party will provide the same level of data protection as required by the framework.
- **Monitoring and Enforcement**: Organizations must take reasonable and appropriate steps to ensure that third-party recipients effectively process the personal data in compliance with the principles. If a third party fails to meet these obligations, the transferring organization must take steps to stop and remediate unauthorized processing.

4. Recourse, Enforcement, and Liability
To ensure effective protection of individuals' privacy rights, the Swiss-U.S. DPF requires organizations to provide recourse mechanisms:

- **Independent Recourse Mechanism**: Organizations must provide accessible, affordable, and independent mechanisms for resolving disputes and complaints regarding their data processing practices. These mechanisms can include cooperation with the Swiss Federal Data Protection and Information Commissioner (FDPIC) or independent dispute resolution bodies in the U.S. or Switzerland.
- **Verification and Compliance Monitoring**: Organizations must verify their compliance with the principles through self-assessment or external reviews. They must maintain records of their data protection practices and provide them upon request in the context of compliance investigations or disputes.
- **Liability for Non-Compliance**: Organizations are liable for damages if they fail to comply with the principles, including in cases of improper onward transfers. Enforcement can be carried out by U.S. authorities such as the FTC or DOT, which can take action against organizations for deceptive practices related to their certification under the framework.

5. Limitations and Safeguards
The Swiss-U.S. DPF includes specific limitations and safeguards to balance privacy protections with other legal obligations:

- **Exceptions**: There are limited exceptions where adherence to the principles may be restricted, for instance, when compliance is necessary to meet national security, public interest, or law enforcement requirements. However, these exceptions are narrowly defined to prevent abuse from happening and ensure that privacy rights are not unduly compromised.
- **Necessity and Proportionality**: U.S. organizations are expected to apply these exceptions only to the extent necessary and must demonstrate that any non-compliance with the principles is limited to the minimum required to meet overriding legitimate interests.
- **Higher Protection Standards**: When possible, organizations are encouraged to opt for higher protection standards beyond the minimum requirements, especially when U.S. law or the principles allow for such discretion.

Why is it important for Swiss Firms?
The Swiss-U.S. Data Privacy Framework is crucial for Swiss firms as it provides a reliable and legally compliant mechanism for transferring personal data to the United States, which is essential for businesses that operate internationally. Given the global nature of commerce, many Swiss companies need to share data with U.S. partners, subsidiaries, or service providers. Without a secure and recognized framework, these data transfers could be subject to legal challenges, disruptions, or potential fines, especially given the stringent data protection requirements under Swiss and EU laws. By adhering to the Swiss-U.S. Data Privacy Framework, Swiss firms can ensure that their data transfers meet the necessary privacy standards, reducing the risk of non-compliance and maintaining smooth business operations.

Moreover, compliance with the Swiss-U.S. Data Privacy Framework helps Swiss companies build and maintain trust with their clients and stakeholders by demonstrating commitment to protecting personal data. In an era where data privacy concerns are increasingly prominent, aligning with recognized data protection frameworks not only safeguards legal standing but also enhances a company's reputation as a responsible and trustworthy business partner. This is particularly important in sectors like finance, healthcare, and technology, where the handling of sensitive personal data is routine, and the stakes for privacy breaches are high.

Advice on Using Standard Contractual Clauses (SCCs)
While the Swiss-U.S. DPF offers a new mechanism for data transfers, using Standard Contractual Clauses remains a viable and necessary option for ensuring data protection compliance, especially in scenarios not covered by the framework or in the case the Swiss-U.S. DPF is deemed invalid by a decision by the Court of Justice of the European Union. Here is why and how you should continue to use SCCs:

1. **Additional Protection Layer**: SCCs provide an extra layer of legal protection by setting out the rights and obligations of both data exporters and importers regarding data handling. This is particularly important when dealing with complex data processing chains involving multiple third parties.
2. **Flexibility and Broad Applicability**: SCCs are adaptable and can be used for a wide range of transfers, including those not specifically addressed by the Swiss-U.S. DPF. This makes them suitable for businesses with diverse data transfer needs.
3. **Compliance with Broader Regulations**: SCCs are recognized under the EU General Data Protection Regulation (GDPR) and are a trusted tool for international data transfers beyond the U.S., making them integral for global operations.
4. **Risk Mitigation**: By incorporating SCCs, you reduce the risk of non-compliance and potential penalties associated with data breaches or mishandling of personal data, especially in regions with stringent data protection laws.

Next steps
It is recommended that you review your current data transfer agreements to ensure they comply with the new Swiss-U.S. DPF principles. Where appropriate, continue or implement the use of SCCs to cover all necessary data flows, providing comprehensive protection for your clients' personal data.

CLICK HERE FOR SOURCE ARTICLE

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

Missouri AG Investigates Hack of National Public Data

Missouri AG Andrew Bailey has opened an investigation into Jerico Pictures, Inc. d/b/a National Public Data, a background check data aggregator, over a data breach that has allegedly exposed personally identifiable information of more than 2.9 billion records.

According to the AG's office, it is investigating allegations that the company failed to properly secure and safeguard its data, which allowed a cybercriminal group to gain access to the company's information, extract unencrypted data, and put the database up for sale.

Other AG efforts to protect consumers' data privacy rights, includes the New Hampshire AG's launch of a new data privacy unit, the Texas AG's data privacy initiative, and the partnership between four AGs and the FCC on privacy and data protection issues.

CLICK HERE FOR SOURCE ARTICLE

Illinois Enacts Additional Employee Protections on Employers' E-Verify Use

Illinois Governor JB Pritzker has signed an amendment to the Illinois Right to Privacy in the Workplace Act that provides additional employee protections regarding employers' use of E-Verify. The amendment's effective date is Jan. 1, 2025, and applies to both private and public employers.

Illinois already had specific rules to ensure that E-Verify is used correctly and fairly. Illinois already:

- Urged employers to consult the Illinois Department of Labor (IDOL) website for current information regarding the accuracy of the program
- Encouraged employers to review and understand their legal responsibilities under E-Verify
- Required all those who administer E-Verify to complete Computer Based Training
- Required employers to post an E-Verify poster in the workplace in both English and Spanish
- Required notification to an employee in writing of a receipt of a Tentative Nonconfirmation Notice (TNC) and their rights to contest the TNC
- Made it clear that an employee could not be terminated prior to receiving a final nonconfirmation notice from the Social Security Administration or the DHS
- Admonished employers to safeguard the information in the system

The amendment continues along the same lines with more specific requirements regarding rights and protections for workers. These include specific notice posting requirements and specific timing on notices to employees about TNCs or upcoming I-9 inspections. Additionally, under the amendment, employees may have representation in meetings regarding TNCs.

The purpose of the amendment may be to ensure employers in Illinois do not exceed federal E-Verify regulations and requirements and treat all employees respectfully by providing sufficient notice of upcoming investigations or TNCs so the employees can plan accordingly.

Some commentators have noted, however, that the new law could be read to prohibit or at least discourage employers from using E-Verify unless required to use it by federal law.

That interpretation is concerning. The amendment adds penalties for violations of the notice provisions that include actual damages plus costs and reasonable attorney's fees for willful and knowing violations. Although IDOL usually attempts to resolve violations through mediation, IDOL and individual complainants can commence actions in court.

We expect IDOL to issue new guidance before the effective date.

CLICK HERE FOR SOURCE ARTICLE

Illinois Employment Law Update Series: Illinois Will Require Pay and Benefits Transparency in Job Postings Beginning January 1, 2025

It is a busy time for employment-related legal updates in Illinois, with Governor J.B. Pritzker recently approving various laws that expand employee protections and add new obligations for employers. Laws Illinois employers need to consider as we move toward 2025:

- amendments to the Illinois Day and Temporary Labor Services Act, which modify and build on 2023 amendments regarding equal pay and benefits for temporary workers (effective 8/9/24) (Client Alert here);
- amendments to the Illinois Human Rights Act expanding the statute of limitations to 2 years and adding new protected classes (effective 1/1/25);
- amendments to the Illinois Human Rights Act, which prohibit the discriminatory use of artificial intelligence and require employer notice of AI use in the workplace (effective 1/1/26);
- amendments to the Illinois Equal Pay Act governing pay transparency in job postings (effective 1/1/25);
- amendments to the Illinois Wage Payment and Collection Act, which expand pay stub requirements (effective 1/1/25);
- expanded scope of documents and protections under the Illinois Personnel Records Review Act (effective 1/1/25);
- a new Illinois Worker Freedom of Speech Act, which protects employees who decline to participate in certain employer-sponsored meetings on religious or political matters (effective 1/1/25);
- amendments to the Illinois Biometric Information Privacy Act, which limit damages for BIPA violations, among other things (effective 8/2/24); and
- amendments to the Illinois Right to Privacy in the Workplace Act, which regulate employer use of E-Verify and similar systems (effective 1/1/25).

Illinois Equal Pay Act Amendments Requiring Pay Scale and Benefits Disclosures in Job Postings

Effective January 1, 2025, Illinois will join an increasing number of states that require employers to list pay ranges in job postings. The amendment (Public Act 103-0539) to the Illinois Equal Pay Act (the "Act") requires all employers with 15 or more employees to include pay scale and benefits information in all open job postings for positions that will be physically performed at least partly in Illinois *and* positions where the employee will report to a supervisor, office, or worksite in Illinois. This means the new requirements will apply to positions where employees will be working remotely from Illinois, as well as positions where remote employees report to a supervisor or location in Illinois.

Key highlights to the amendment include:

Required Pay Scale, Benefits, and Other Compensation Disclosures

"Pay scale and benefits" is defined as the wage or salary, or the wage or salary range, and a general description of the benefits and other compensation. This includes, but is not limited to, bonuses, stock options, or other incentives the employer "reasonably expects in good faith" to offer for the position. The amendment provides that employers should set the position's reasonably expected pay scale and other compensation by reference to "any applicable pay scale, the previously determined range for the position, the actual range of others currently holding equivalent positions, or the budgeted amount for the position, as applicable."

To satisfy the pay scale and benefits disclosure requirement, employers may include the pay scale and benefits information directly in a job posting *or* post a hyperlink to a publicly viewable webpage that includes the relevant pay scale and benefits information. Employers also may satisfy the benefits disclosure requirement by referring in the job posting to a relevant and up-to-date general benefits description in an easily accessible, central, and public location on the employer's website.
Significantly, the amended Act does not require employers to post job openings. However, if an employer or employment agency does not post pay scale and benefits information, it must provide applicants with the pay scale and benefits information at the applicant's request and prior to making a job offer or discussing compensation for the position. The amendments confirm that employers and employment agencies are not prohibited from asking applicants about their wage or salary expectations for a position.

Third Party Postings

Employers using one or more third parties to publish job postings must provide the third party with the pay scale and benefits information (or hyperlink) to include in the job posting. Notably, the amended Act allows for liability against third parties

for failing to include the pay scale and benefits information in the job posting unless the third party can show that the employer failed to provide the necessary pay scale and benefits information.

Promotion Postings
An employer must announce, post, or otherwise make known all opportunities for promotion to all current employees within 14 calendar days after the employer makes an external job posting for positions, except for designated positions that are exempt from competitive selection.

Record Keeping and Nondiscrimination Protections
Employers must make and maintain records regarding each job position's pay scale and benefit information and any related job posting for at least *five (5) years*. Furthermore, employers and employment agencies cannot discriminate or retaliate against applicants or employees for exercising any rights under the law.

Illinois Department of Labor Complaints and Investigations
The Amended Act provides that the Illinois Department of Labor (IDOL) may investigate a complaint from any person who claims to be aggrieved by an employer's or other third party's failure to comply with these new job posting requirements. A complaint must be filed with the IDOL within one year of the alleged violation.

If the IDOL determines that an employer has failed to comply with the Act's new pay transparency requirements, it can issue a notice of violation and impose fines ranging from $250 to $10,000, depending on the number of prior employer violations, whether the job posting is active at the time the IDOL issues its notice of violation, whether the position has been filled, and other factors. For job postings that are still open, cure periods are available to first- and second-time offenders. There are no similar cure periods provided if the job posting is no longer active at the time the IDOL issues its notice of violation. A job posting found to violate the Act shall count as one job posting, regardless of the number of duplicative postings.

Takeaways
It is recommended that employers and employment agencies begin reviewing their existing job postings and consult their employment counsel to ensure compliance with these new pay transparency requirements before the end of the year.

CLICK HERE FOR SOURCE ARTICLE

Illinois Passes Artificial Intelligence (AI) Law Regulating Employment Use Cases

Illinois joins other states, including Utah and Colorado, in passing its own legislation to regulate AI. On August 9, 2024, Illinois Governor JB Pritzker signed a new bill into law (HB 3773) that amends the Illinois Human Rights Act (IHRA) to address the risks associated with AI use in the employment context. The amendment affects any employer who currently uses, or intends to use, AI, including generative AI, to make decisions around recruitment, hiring, promotions, renewal of employment, training, discipline, discharge, or any other term or condition of employment. Under the new amendment, employers are prohibited from using AI in a manner that causes a discriminatory effect for any protected characteristic already covered under the IHRA or zip codes as a proxy for a protected class under the IHRA. Employers are also required to give notice if they are using AI.

Background
HB 3773 amends the IHRA, which applies to employers who employ one or more employees within Illinois during 20 or more calendar weeks a) within the calendar year of or b) preceding the alleged violation. Under the IHRA, protected characteristics include race, color, ancestry, national origin, disability, religion, sex, sexual orientation, pregnancy, military status, military discharge, age (over 40), order of protection status, marital status, citizenship, work authorization status, language, conviction record, and arrest record. Beginning January 1, 2025, the IHRA will also protect "family responsibilities" and "reproductive health decisions."

"AI" Definition
"Artificial intelligence" is defined consistent with leading AI laws—such as Colorado's Concerning Consumer Protections in Interactions with Artificial Intelligence Systems and the EU AI Act—to mean any "machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content,

recommendations, or decisions that can influence physical or virtual environments." The amendment also covers generative AI (i.e., AI that is capable of generating text, images, audio, videos, or other content that would otherwise be produced by humans).

Detailed Guidance on Affirmative Steps Lacking

Illinois's amendment comes on the heels of Colorado passing its AI law in May 2024, which also addresses algorithmic discrimination, and New York City's Local Law 144, which requires employers to conduct, among other things, bias audits. However, unlike the AI laws in Colorado and New York City, Illinois's does not provide detailed guidance regarding affirmative steps employers are required to take to address discriminatory outcomes, such as bias audits, AI impact assessments, and implementing risk management systems.

Discriminatory Effect Prohibited and Notice Requirement

The law covers AI that has the effect of discriminating against employees based on protected characteristics, regardless of whether the discrimination was intentional. Employers are also required to notify employees if the employers use AI for the purposes mentioned above. While the law does not specify the exact form this notice must take, the Illinois Department of Human Rights will adopt rules to define the circumstances and conditions that would trigger a notice requirement, a timeline for the same, and a means of providing that notice.

Enforcement and Remedies

The Illinois Department of Human Rights and Illinois Human Rights Commission will enforce the law, and employees can file a charge with the Department of Human Rights if they believe they have been discriminated against due to AI. Remedies may include back pay, reinstatement, emotional distress damages, and attorneys' fees.

Takeaways

Based on the latest legislative developments, Illinois's AI law underscores that use of AI in the employment context carries higher risks. Employers that are considering using AI for recruiting or other human resources-related decisions should consider conducting a bias audit on their AI systems and/or conducting sufficient diligence on the AI vendor providing such a tool. Those assessments should look at whether AI tools disproportionately impact certain groups—such as those of a certain race, gender, or age. Employers should document their analysis in an AI-impact assessment, keep records of any formal audits conducted on the AI system, and continuously monitor the AI system once it is used in the real world in order to make adjustments if the AI system deviates. Finally, employers should be transparent about their use of AI through appropriate AI pre-use notices.

CLICK HERE FOR SOURCE ARTICLE

Maryland Department of Labor Issues Highly-Anticipated Guidance on New Wage Transparency and Paystub Notice Obligations

As most employers with Maryland employees (hopefully) know, starting October 1, 2024, they are subject to new wage range posting and paystub notice obligations, as detailed in our April 10, 2024 E-lert on new Maryland employment laws. The Maryland Department of Labor promised to release guidance to help employers in complying with these new obligations, for which employers have been waiting with bated breath. And it is finally here! The MDOL has included this information, along with other information on existing wage laws, on a new Wage and Hour webpage.

Background on Wage Transparency Requirement. Maryland's Equal Pay for Equal Work Act currently requires employers to provide the wage range for the position in question only upon an applicant's request. The new law now imposes more expansive obligations, including the following:

- Posting Requirement: Employers must include the following in any internal or external job posting:
  - the wage range,
  - a general description of benefits, and
  - any other applicable compensation.

If the posting is not available to the applicant, it must be provided to the applicant before any discussion of compensation is held with the applicant and at any other time on request of the applicant.

- Record Retention Requirement: Employers must retain records of compliance for at least three (3) years.
- "Wage range" is defined as the minimum and maximum hourly rate or salary, set in good faith by reference to one

of the following:

- any applicable pay scale;
- any previously determined minimum and maximum hourly rate or salary for the position;
- the minimum and maximum hourly rate or salary for an individual holding a comparable position at the time of the posting; or
- the budgeted amount for the position.

In addition, employers may not refuse to promote or transfer an employee, or refuse to interview, hire or employ an applicant, because the employee/applicant refused to provide their prior wage history (in accordance with the existing salary history ban), asked for the wage range, or exercised any other rights under the law.

Fortunately for employers, the law does not allow individuals to bring their own lawsuit against the company. Employees and applicants may only file a complaint with the Commissioner of Labor and Industry, who may order compliance and impose a civil penalty.

The Wage Transparency Guidance: As to the wage transparency requirement, the MDOL has provided the following resources:

- Wage Range Transparency FAQs
  - Narrative Examples
  - Compensation Disclosure Form (PDF)
  - Compensation Disclosure Form Instructions (PDF)

Notably, if the employer uses the MDOL's form, it will be deemed to be in compliance with its posting obligation under the law. However, an employer is not required to use the form and the MDOL also provides other narrative examples of postings which are also compliant under the law.

The FAQs also provide further clarity and examples regarding which postings would be covered. Below are some notable things specified in the FAQs:

- A posting for a position that would only occasionally perform work in Maryland is not covered under the law. Specifically, the MDOL provides examples of occasional work as attending meetings and conferences or communicating with Maryland employees.
- A separate range of pay must be provided for each location or opportunity, if the posting involves multiple locations or multiple opportunities at different levels of seniority.
- The following benefits are required to be listed: employer provided insurance such as health or life or other employer-provided insurance; paid or unpaid time off work such as paid sick or vacation days, or leaves of absence; retirement or savings funds such as 401(k) plans or employer-funded pension plans; or other forms of compensation such as the value of employer-provided meals or lodging.
- Employers are required to include any "any other compensation offered." Some examples of any other compensation offered include: overtime, compensatory time, differentials, premium pay, tips, commissions, bonuses, stock or stock options, and any portion of service charges.
- Employers are required to provide the required disclosure when reposting a position; however, the employer may change the terms, if in good faith. For example, a change of the terms may be needed to attract more applicants to the position.

Background on the Paystub Notice Requirement. Currently, at the time of hiring, employers must give notice regarding the rate of pay, the regular paydays, and leave benefits. They must also provide for each pay period a statement of the employee's gross earnings and any deductions.

The new law makes clear that these notices must be in writing. In the case of the pay period statements, the required information must be on the physical pay stub or the online pay statement. The new law also greatly expands the information that must be provided each pay period to specifically include the following:

- The employer's name as registered with the State, address and telephone number;
- The date of payment and the beginning and ending dates of the pay period for which the payment is made;

- For non-exempt employees, the number of hours worked in the pay period;
- The rates of pay;
- The gross and net pay earned during the pay period;
- A list of additional bases of pay, including bonuses, sales commissions, or anything else; and
- For piece-rate employees, the applicable piece rates of pay and number of pieces completed at each rate.

Similar to the wage transparency law, there is no ability for an employee to sue for violations. But if an employer fails to comply, the Commissioner of Labor and Industry may order the employer to provide the required information and impose an administrative penalty of up to $500 for each employee who did not receive the required notice. Employers may appeal an order by requesting an administrative hearing. If an employer fails to comply with the order, the Commissioner can bring suit against the employer for enforcement.

The Paystub Notice Guidance: As to the paystub notice requirement, the MDOL has provided the following resources:

- Pay Statement FAQs
- Pay Stub Template
- Pay Statement Template Instructions

Similar to the Wage Transparency Guidance, if the employer uses the MDOL's template for the paystub notice, that will be considered compliance with the law.

The FAQs also clarify several things:

- Workers cannot waive the written notice requirements.
- If an employee receives different rates of pay or multiple bases, all must be reported on the employee's pay statement.
- If an employee's rate of pay is changed, the employer must provide at least one pay period of advance notice prior to any decrease. However, advance notice is not needed by an employer for an increase.
- The Tip Credit Wage Statement, which is required for restaurant employers, is not sufficient to meet the requirements of this law. However, the elements required in the Tip Credit Wage Statement can be included in the pay stub.

CLICK HERE FOR SOURCE ARTICLE

New California Law Will Require AI Transparency and Disclosure Measures

On September 19, 2024, California Governor Gavin Newsom signed into law the California AI Transparency Act, which will require providers of generative artificial intelligence (AI) systems to: (a) make available an AI detection tool; (b) offer AI users the option to include a manifest disclosure that content is AI generated; (c) include a latent disclosure in AI-generated content; and (d) enter into a contract with licensees requiring them to maintain the AI system's capability to include such a latent disclosure in content the system creates or alters. The California AI Transparency Act goes into effect January 1, 2026, and is the nation's most comprehensive and specific AI watermarking law.

Key Definitions

The law's provisions apply to "covered providers," defined to mean "a person that creates, codes, or otherwise produces a generative artificial intelligence system that has over 1,000,000 monthly visitors or users and is publicly accessible" within California. Additionally, a "generative artificial intelligence system" is defined as:

An artificial intelligence that can generate derived synthetic content, including text, images, video, and audio, that emulates the structure and characteristics of the system's training data.

The law also defines "artificial intelligence" to mean:

An engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

Covered providers will be required to comply with the law as of the date it goes into effect; i.e., January 1, 2026.

Requirements for Covered Providers

The law's transparency requirements will require covered providers to make disclosures about the use of generative AI systems. First, covered providers will be required to make available—at no cost to a user—AI detection tools that will allow users to assess whether image, video, or audio content has been created or altered using a generative AI system. Subject to certain technical requirements and privacy protections, these tools will also be required to provide system provenance data regarding the content, in order to allow users to verify the devices, systems, or services used to generate such content and content authenticity.

Additionally, covered providers will be required to provide users with both "latent" disclosures in AI-generated content and an option of including a "manifest" disclosure in such content. Manifest disclosures—meaning disclosures on AI-generated content that are easily perceived, understood, or recognized by a natural person—will be required to identify the content as AI-generated in a clear, conspicuous, appropriate, and permanent manner. Latent disclosures—those that are not manifest, but are instead present in the metadata of AI-generated content—will be required to convey (to the extent technically feasible and reasonable, either directly or through a link to a permanent website) the covered provider's name, the name and version number of the generative AI system, the time and date of the content's creation or alteration, and a unique identifier. The latent disclosures must also be detectable by the AI detection tool, consistent with widely accepted industry standards, and must be either permanent or extraordinarily difficult to remove.

Finally, covered providers that license their generative AI systems to third parties will be required to ensure that licensees maintain these disclosure requirements. If covered providers know that third-party licensees are not capable of including such disclosures, they will be required to revoke their licenses within 96 hours.

The law will be enforced by the California Attorney General, a city attorney, or a county counsel, and provides for civil penalties of $5,000 per day if a covered provider is found to be in violation.

Takeaways for Interested Parties

California joins Colorado, Utah, and Illinois in requiring transparency regarding the use of AI. However, unlike those other states, California's law is the first AI law to create comprehensive and specific requirements related to watermarking. Companies developing generative AI systems should be mindful of these specific technical requirements as they invest time and resources developing technology within scope of this law. Licensors and licensees of cover AI systems should consider updating their agreements to address these contractual requirements.

CLICK HERE FOR SOURCE ARTICLE

Massachusetts Enacts Salary Transparency Law

On July 31, 2024, Massachusetts enacted a new law entitled An Act Relative to Salary Range Transparency, which requires employers disclose a pay range in job postings and advertisements. The law is slated to become effective July 31, 2025, and applies to Massachusetts employers with 25 or more employees. Massachusetts is the latest among several states, such as California, New York, and Connecticut, to enact payroll transparency requirements for employers.

Under the new law, employers must include the "annual salary or hourly wage range that an employer reasonably and in good faith expects to pay for the position" in the posting or advertisement. The pay range must be shared not only in the job posting but must also be provided to an employee or applicant upon request in relation to a current or new position, a promotion, a transfer, or a job offer.

The law contains an anti-retaliation provision, prohibiting covered employers from discharging, retaliating, or discriminating against any employee or applicant who exercises their rights under the Act. The law, however, does not contain a private right of action and the Massachusetts Attorney General's Office is tasked with enforcing its provisions. Violators of the law may be subject to fines.

In addition, the law requires Massachusetts employers with over 100 employees to file an annual wage data report with the Secretary of the Commonwealth, including race, ethnicity, sex, and job category. This reporting requirement takes effect February 1, 2025.

Employers should consult with counsel to ready for compliance, including preparing required salary range information for future job postings and training human resources personnel on the law's requirements. Likewise, Massachusetts employers with at least 100 employees should work with counsel on the preparation and filing of the required wage data report.

CLICK HERE FOR SOURCE ARTICLE

Pay Transparency Comes to Minnesota

Pay transparency laws are increasingly being implemented across the United States with a purported goal of increasing fairness, addressing wage inequalities and promoting a more transparent hiring process. A dozen states and the District of Columbia have passed some form of a pay transparency law in recent years. The Minnesota legislature passed its own version of a pay transparency law this year with an effective date of January 1, 2025.

Requirements of the Law

Under the new Minnesota law, employers with 30 or more employees at one or more sites in Minnesota must provide the minimum and maximum annual starting salary or hourly range of compensation, compliant with the following rules:

- The range may not be open ended.
- The range must be based on a "good faith estimate."
- If the position does not have a range, a fixed pay rate must be listed.

Employers must also provide a general description of all benefits and other compensation, including health or retirement benefits.

Scope of the Law

These requirements apply to "any solicitation intended to recruit job applicants for a specific available position." This includes any electronic or hard copy posting, and its scope extends to all external or internal-facing job postings.

Employer's Next Steps

In advance of the January effective date, all employers who have Minnesota employees or recruit in Minnesota should ensure that their job postings comply with the new law and that any third-party vendors they use to facilitate job postings are likewise in compliance. Employers should also be aware that Minnesota's wage disclosure protections for applicants remain in effect and prevent an employer from requiring an applicant to provide their salary history or even asking, encouraging or prompting an applicant to disclose their pay history for the purpose of negotiating wages, salary, benefits or other compensation.

Multi-state employers need to prepare for pay transparency laws in other states, as well. Illinois, Maryland, Massachusetts and Vermont have recently passed pay transparency laws, and each state has slightly different requirements for employers to meet.

CLICK HERE FOR SOURCE ARTICLE

Amendments Align Pennsylvania's Breach Notification Law with Majority of States

Earlier this year, Governor Josh Shapiro signed amendments to Pennsylvania's Breach of Personal Information Notification Act (BPINA) into law, which go into effect on September 26. As part of the implementation of these requirements, Pennsylvania Attorney General (AG) Michelle Henry announced the launch of an online portal for companies and other entities to report data breaches that impact more than 500 Pennsylvania residents. As with notification to impacted individuals, covered entities must notify the AG "without unreasonable delay." This new requirement aligns Pennsylvania's data breach notification law with the 35 states that have existing notice requirements for the applicable state regulator when a threshold number of state residents are impacted. Many of these states utilize a similar portal for submissions for ease of reporting.

The portal is available here. The AG's website also provides guidance on the process to submit required information about

the breach, and information about the BPINA for entities and residents.

In addition to the regulatory reporting requirement, the amendments provide protections for types of information that up until now remained unprotected under the BPINA. As with the previous version of the BPINA, notification to individuals is triggered when a data breach involves a person's name and Social Security number, financial account number, and driver's license or state ID number. The amendments now add protections for an individual's name in combination with medical information in the possession of a state agency or state agency contractor, health insurance information, or a username and password that permits access to an online account as newly protected data elements that also trigger notice to individuals if impacted. However, impact to these data elements only triggers notification where the covered entity reasonably believes the unauthorized access or acquisition of the information has caused, or will cause, loss or injury to any Pennsylvania resident. Pennsylvania also joins five other states in requiring entities provide impacted individuals with 12 months of credit monitoring when an individual's Social Security number, driver's license number, state ID number, or bank account number is impacted.

Why It Matters

Prior to the BPINA amendments, Pennsylvania was among the 15 states that do not mandate organizations suffering a qualifying breach of consumer personal identifying information to notify the relevant state regulator. Given the new protections for additional types of information and the regulatory reporting requirements, organizations handling personal information of Pennsylvania residents should revise their incident response plans. These changes could subject organizations to increased regulatory scrutiny. Failure to comply with these new requirements may be deemed a violation of BPINA, constituting an unfair or deceptive act or practice in violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, and subject companies to injunctive relief or monetary penalties.

The BPINA amendments add to the mosaic of breach notification laws across all 50 states, with applicability based on the impacted individual's state of residence. While these amendments aim to align Pennsylvania law with other state data breach notification laws, they also highlight the diverse requirements that can complicate compliance in the wake of a cybersecurity incident, particularly for companies that operate in multiple jurisdictions. Engaging experienced counsel after a security incident is always a best practice to help navigate the obligations under the patchwork of state regulatory frameworks.

CLICK HERE FOR SOURCE ARTICLE

COURT CASES

Employer Zero-Tolerance Marijuana Policy Justified Termination, Federal District Court Agrees

Zero-tolerance marijuana policies are not unlawful in Illinois, a federal district court has determined, providing greater clarity for employers. In late 2019, Illinois amended its marijuana law, the Cannabis Regulation and Tax Act (CRTA), to ensure employers could continue to implement policies prohibiting workers from using marijuana or marijuana products despite the state's decision to permit adult recreational marijuana use. Nevertheless, the extent to which employers could enforce their policies and possible conflicts with Illinois's law prohibiting discipline for lawful non-work activities remained.

A new court decision—*White v. Timken Gears & Services, Inc.*, No. 21-cv-2290 (N.D. Ill. July 17, 2024)—has answered some of these questions, providing further support for Illinois employers that have adopted and want to continue to enforce zero-tolerance policies regarding marijuana.

Background

Employer policy prohibited marijuana and required random testing

The employer company develops, manufactures, and sells industrial motion products, such as augers, gear drives, and transmissions. The company implemented a Drug and Alcohol Policy that prohibited the unlawful manufacture, distribution, dispensation, possession, or use of controlled substances or alcohol in the workplace. The policy defined "controlled substances" to include marijuana.

The employer also required employees at its manufacturing and distribution centers to undergo random drug screenings. The policy provided that an employee, upon a first-time positive test result, would be required to participate in counseling, stop using the substance for which they tested positive, and submit to unannounced follow-up testing. A second positive result would subject that employee to immediate termination of employment.

Employee tested positive for marijuana and participated in the Employee Assistance Program
The plaintiff-employee worked for the employer as a Territory Account Manager. In that role, he worked from home selling products and repair services, but also drove a company car to customers' facilities.

On December 6, 2019, the employee tested positive for marijuana on a random drug test. He participated in the employer's Employee Assistance Program and continued to work during that time, except he was not allowed to drive a company vehicle.

Employee tested positive for marijuana in follow-up testing

On January 6, 2020, the employee was required to submit to a follow-up drug test, and his result was negative. On January 21, 2020, the employee was required to take another drug test, and this time his result was deemed a "negative dilute," which the employer treated as a failed test. The employee was allowed to take a re-test, and his result was again deemed a "negative dilute." The employer was unable to reach the employee via phone afterward, and the employee did not respond to the company's email to him. On January 27, 2020, the employer permitted the employee to undergo a second re-test, and his result was positive for marijuana. As a result, the employer terminated the employee's employment citing his violation of the Drug and Alcohol Policy.

Employee sues for alleged violation of the Illinois Right to Privacy in the Workplace Act (IRWPA)

The employee filed suit against the employer for allegedly violating the IRWPA, 820 ILCS 55/1, *et seq.* and the case was removed to the U.S. District Court for the Northern District of Illinois.

The IRWPA prohibits an employer from firing an employee "because the individual uses lawful products off the premises of the employer during nonworking and non-call hours." 820 ILCS 55/5(a). As of January 1, 2020, cannabis is a "lawful

product" under the IRWPA.

However, Illinois's Cannabis Regulation and Tax Act (CRTA) addresses employment and employer liability for conduct relating to the use of cannabis under state law. Section 10-50 specifically addresses what actions employers can take regarding cannabis-related violations. Those provisions were central to the court's analysis of the employee's claims against the employer.

Court's analysis of CRTA's employment provisions

Engaging in statutory interpretation, the court identified three key provisions from Section 10-50 of the CRTA. First, the CRTA authorizes employers to adopt two types of drug policies: "zero tolerance or drug free workplace policies" or "employment policies . . . concerning [conduct] in the workplace or while on call." The court emphasized that the CRTA authorized adoption of *either* type of policy and that a "zero tolerance" policy need not be limited to employees "in the workplace."

Second, the CRTA states that employers may discipline or discharge an employee for violating their "employment policies or workplace drug policy." The court stated that this provision "not only authorizes employers to adopt drug policies, but it also authorizes employers to terminate employees for violating them."

Third, the CRTA precludes employees from bringing claims against an employer for certain actions taken pursuant to their drug policies, including "reasonable and nondiscriminatory random drug testing." The court stated: "A plain reading of this provision . . . indicates that an employer may enforce its drug policies through random drug testing so long as the testing is (1) reasonable and (2) nondiscriminatory."

The court summarized these provisions as follows: "[E]mployers may adopt a zero tolerance or drug free workplace policy; zero tolerance or drug free workplace policies need not be tied to 'in the workplace' conduct; such policies may be enforced through reasonable and nondiscriminatory random drug testing; and an employee may be terminated for violating the employer's drug policy."

Court approves the company's zero-tolerance policy and random drug testing

Applying this interpretation to the case at hand, the court determined that the employer had adopted a permissible "zero-tolerance" policy that it enforced through random drug testing. Therefore, in order to prove a violation of the CRTA and, in turn, the IRWPA, the employee needed to show that the employer's actions were either discriminatory or unreasonable. The court concluded that the employee had not made such a showing and therefore granted summary judgment in the employer's favor.

Explaining its reasoning, the court observed that the employer had not selected the employee for testing based on a legally protected characteristic, so the employer's policy and enforcement could not be discriminatory. As for reasonableness, the court noted that the employee had acknowledged receipt of the employer's Drug and Alcohol Policy, which advised him of the company's drug testing procedures and potential consequences for violating the policy.

The court also noted that the employer did not immediately terminate the employee for a first-time positive test result and "[c]ritically" allowed the employee to provide a negative test result before conducting additional, follow-up testing. After further observing that the employer granted the employee more chances to comply than its policy than required, the court concluded that both the employer's policy and its implementation of the policy were reasonable.

Because the employer's policy and actions were neither discriminatory nor unreasonable, the court held that the CRTA allowed the employer's actions resulting in the termination of the employee's employment and the employee could not maintain a claim against the employer under the IRWPA.

Conclusion

Illinois is one of numerous states that has legalized recreational marijuana. Despite early uncertainty regarding the interpretation of Illinois' laws around marijuana use, the courts' interpretations have helped clarify that employers can still

implement drug-free workplace polices, including zero-tolerance policies, and enforce them, including by requiring random drug testing. The *Timken* case further demonstrates that Illinois employers' zero-tolerance policies are not restricted to prohibiting only in-the-workplace conduct, and adverse action can occur as long as it is not unreasonable or discriminatory. Still, employers are well advised to closely review their drug-free workplace and testing policies and, if necessary, revise to ensure that employees are aware of the employer's expectations regarding drugs, including marijuana, and potential consequences of a policy violation.

CLICK HERE FOR SOURCE ARTICLE

An Employee's Off-Duty Social Media Posts Can Constitute Workplace Harassment

As the workplace continues to take a new shape, the distinction between "workplace conduct" and "off duty" conduct continues to fade for many. After a recent Ninth Circuit ruling, employers must be more vigilant than ever in monitoring and responding to employee social media postings, even when they are personal and "off duty."

After plaintiff made numerous complaints and reported these posts to her supervisor and other prison officials, the prison directed her co-worker to stop posting offensive conduct in accordance with the prison's anti-harassment policy. Despite this instruction, the Lieutenant continued to regularly post offensive material, including suggestions of sexual relations with female co-workers. The plaintiff eventually resigned and filed a lawsuit asserting a claim of sex discrimination under Title VII. But a lower court threw the case out finding that the prison was not legally responsible for the Lieutenant's conduct when it "occurred entirely outside of the workplace."

On appeal, the Ninth Circuit reversed, holding that regardless of where the Lieutenant was when he posted the offensive content, his colleagues viewed the content, and it had the effect of creating a hostile work environment. The Ninth Circuit highlighted that the important question was not whether the Lieutenant posted from the physical workplace, but whether his conduct had an unreasonable effect on plaintiff's work environment. Under that 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 manner" because "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's holding is consistent with the EEOC's recently issued Enforcement Guidance on Harassment in the Workplace, which we previously wrote about here. There, the EEOC states that conduct can affect the terms and conditions of an employee's employment "even if it does not occur in a work-related context."

Takeaways for Employers

- The lines between the workplace and "outside the workplace" continue to blur. Employers should be prepared to respond to their employees' offensive online content irrespective of when and where it was posted.
- Employers should develop or revise policies providing for swift and thorough investigations into employee claims of misconduct, including claims involving social media posts.
- Employers should consider revising any relevant training materials for supervisory employees relating to "offsite" or "off duty" conduct and harassment.
- Employers should also consider revising any relevant policies on harassment to include provisions relating to out of work conduct and social media usage, to ensure employees are on notice that their social media postings may impact their employment.
- Employers should work with counsel to ensure they are mindful of statutory protections of lawful and political off-duty employee conduct, which some coworkers may subjectively perceive as offensive. More on that here.

CLICK HERE FOR SOURCE ARTICLE

The DOJ's Lawsuit Against RealPage: Unpacking the Allegations and Implications for the Rental Market

The U.S. Department of Justice (DOJ) and eight state attorneys general have filed a lawsuit against real estate software company RealPage, alleging that its algorithmic pricing system has contributed to widespread price-fixing among landlords, harming millions of American renters. RealPage is an American company that provides property management software for multifamily, commercial, single-family and vacation rental housing industries. The lawsuit underscores growing concerns

over the use of artificial intelligence (AI) and algorithmic decision-making in critical markets, including housing.

The Core Allegations

The DOJ's antitrust suit centers on RealPage's YieldStar software, a tool used by landlords and property managers to set rental prices. The software analyzes various data points, including local market trends, vacancy rates and rental history, to recommend what landlords should be charging in rent. However, the DOJ contends that the software goes beyond merely providing recommendations; it allegedly encourages and facilitates collusion among landlords, leading to artificially inflated rents.

According to the DOJ, RealPage's software enables landlords to coordinate pricing strategies in a manner that violates federal antitrust laws. By relying on the same algorithmic recommendations, landlords can collectively set higher prices, effectively reducing competition and harming renters. The lawsuit argues that this practice constitutes illegal price-fixing and has contributed to the ongoing housing affordability crisis in the United States.

The Broader Implications

The lawsuit against RealPage raises broader questions about the role of AI and algorithmic decision-making in markets that impact millions of people. While algorithms can enhance efficiency and optimize pricing, they can also create unintended consequences when used inappropriately or without adequate oversight.

In the case of RealPage, the DOJ alleges that the company's software has created a de facto cartel among landlords, where competition is stifled, and renters bear the brunt of the consequences. This case could set a precedent for how AI-driven tools are regulated, especially in sectors like housing.

RealPage's Response

In response to the lawsuit, RealPage has denied any wrongdoing, arguing that its software simply helps landlords make data-driven decisions in a competitive market. The company claims its tools are designed to reflect market conditions and optimize occupancy rates, not to engage in price-fixing. RealPage also asserts that its software provides valuable insights that help landlords manage properties more efficiently, ultimately benefiting tenants by ensuring the long-term viability of rental properties.

Despite these claims, the DOJ's lawsuit highlights the need for greater scrutiny of algorithmic pricing tools, especially when they have the potential to impact millions of people. As the case unfolds, it will likely spark a broader debate about the ethical and legal implications of AI in the rental market and other industries.

The Path Forward

The outcome of the DOJ's lawsuit against RealPage could have far-reaching implications for the rental market and the regulation of AI-driven pricing tools. If the court rules in favor of the DOJ, it could lead to increased regulation of similar technologies, particularly in markets where consumers are vulnerable to price manipulation.

In the meantime, renters, landlords and policymakers alike will be watching this case closely. For landlords and property managers, it serves as a reminder of the legal risks associated with relying too heavily on algorithmic tools without considering their broader impact.

As AI continues to permeate various aspects of daily life, cases like this one will likely become more common, prompting ongoing discussions about the balance between innovation, competition and consumer protection. The RealPage lawsuit may be the first of many legal challenges that seek to define the boundaries of algorithmic pricing and its role in the modern economy.

CLICK HERE FOR SOURCE ARTICLE

Remember that It's Easier to Prove Retaliation than Harassment.

As most employers know, Title VII prohibits not only discrimination or harassment based on race, ethnicity, religion or gender, but also retaliation for opposing any unlawful practice (e.g. complaining about discrimination or harassment). But the standards for proving each are different, and a recent case from the U.S. Court of Appeals for the First Circuit reminds employers that a lower standard of proof applies to retaliation cases.

In *Stratton v. Bentley University*, the employee asserted various discrimination claims as well as a retaliation claim. The federal district court granted summary judgment for the employer, finding that, even assuming all facts in the employee's favor, the employee's claims had no merit as a matter of law. On appeal, the First Circuit affirmed the district court's decision, but took the opportunity to clarify the standard that applies to retaliation claims.

In order to succeed on a retaliation claim, a plaintiff must show that (1) they engaged in protected activity; (2) they suffered some materially adverse action; and (3) the adverse action was causally linked to their protected activity. Previously, in order to establish a materially adverse action, a plaintiff was required to show conduct that was so "severe or pervasive that it materially altered the conditions of her employment." However, in *Burlington N. & Santa Fe Ry. Co. v. White*, the U.S. Supreme Court set forth the appropriate standard for materially adverse actions in the context of retaliation claims, finding that they are not limited to actions affecting the terms and conditions of employment. Rather, it covers actions that "could well dissuade a reasonable worker from making or supporting a charge of discrimination" – a much lower standard. And the First Circuit clarified that its prior, higher standard was no longer appropriate, and has been replaced with *Burlington-Northern's* "might-have-dissuaded" standard.

In our practice, we often see cases in which an employee is unable to establish that they have been subjected to unlawful discrimination or harassment, but they are able to prove retaliation. So employers must be careful to ensure that the treatment of employees who have complained about discrimination or harassment is legitimate and consistent with the treatment of non-complaining employees.

CLICK HERE FOR SOURCE ARTICLE

Appeals Court: No FCRA Informational Injury Standing

A job applicant who claims he was not fully informed about adverse information that appeared on a background check is not entitled to relief under the Fair Credit Reporting Act (the FCRA), the Sixth Circuit Court of Appeals ruled on Aug. 20. The court cited the Supreme Court's decision in *TransUnion LLC v. Ramirez*, in holding that Thomas Merck was not entitled to relief because he alleged no injury other than a statutory violation of the FCRA. In doing so, the appeals court affirmed the federal district court's granting summary judgment for lack of standing.

Merck had applied for a position at Walmart and was offered a job as long as he had a successful background check. Merck failed to disclose a misdemeanor conviction, which showed up on his background report.

Walmart received a report indicating that Merck failed to disclose a negative item on his job application. Merck, however, received a report stating that he was not competitive for the job, and not disclosing a specific reason why.

Merck filed suit arguing that Walmart violated the FCRA by willfully failing to provide applicants with a full copy of their consumer report before taking adverse action against them.

The appeals court said that Merck had not established an "informational injury" based on *Ramirez*. The court said that even if Merck had had the full information, it would not have helped him, since his application was rejected because he failed to discuss his misdemeanor conviction.

"Merck has failed to point to sufficient evidence of adverse effects to survive summary judgment on his informational-injury theory of standing," the appeals court said.

CLICK HERE FOR SOURCE ARTICLE

INTERNATIONAL DEVELOPMENTS

New Duty to Prevent Sexual Harassment in the UK - Guidance for Employers

Back in June, we highlighted that, from October 26, 2024, all employers in the UK will have a mandatory duty to take "*reasonable steps*" to prevent sexual harassment of their employees in the course of their employment. We explained that we were expecting the Equality and Human Rights Commission (EHRC) to update its existing guidance on sexual harassment to include guidance about the scope of this new duty.

We now have the EHRC's updated guidance (the "Guidance"). There is not a huge amount of detail on the scope of the duty, but here are three key things employers should be aware of:

- The new duty is anticipatory rather than reactive: Employers will be required to carefully assess the risk of sexual harassment happening in their business and actively take steps to prevent it from happening in the future, including analyzing situations where it has happened before. Employers that take a passive or reactive approach to sexual harassment are likely to find themselves in breach of the new duty.
- "Reasonable" is an objective test and will vary from employer to employer but the Guidance has made clear that:
    - Relevant factors will include (for example) the size of the employer, the sector it operates in, the working environment and its resources, the types of third parties employees may come into contact with, level of risk and how effective the step might be when bearing factors like time, cost, and level of disruption in mind. Employers may want to carry out an audit to identify their specific risks and the steps that are likely to be effective to address them. This might include ensuring they have policies and training which is regularly updated.
    - While liability for harassment by third parties was removed at the Bill stage, employers must take reasonable steps to prevent sexual harassment by third parties. Depending on the nature of the employer this might include customers, clients, service users, friends and family of colleagues and/or members of the public.
- The EHRC will have wide enforcement powers: This will include the power to investigate, issue unlawful act notices, enter into legally binding agreements with employers to prevent future unlawful acts and seek injunctions to restrain employers from committing unlawful acts. We will need to wait and see if the EHRC will be given additional resources in order to take enforcement action. However, you should note that:
    - The EHRC will be able to exercise these powers if it suspects there may have been a breach of the new preventative duty – it will not need to wait for an incident of sexual harassment to take place or for an employee bringing a claim.
    - Any enforcement action by EHRC for failing to comply with this duty could lead to reputational damage and so employers will want to take steps that are reasonable to reduce the risk of facing such action in the first place.

What's next?

The EHRC ran a short consultation on the Guidance, which closed on August 6, 2024, and it may issue further updated guidance in light of the responses before the new preventative duty becomes law on October 26, 2024. In the meantime, we recommend that employers start taking steps now to ensure that they are ready to comply from day one. Many businesses will already be taking steps to address sexual harassment, but employers will want to be able to evidence that they have assessed their risk and demonstrate the action they have taken.

Going forward, the new Labour government has indicated that it plans to extend the Act to require employers to take "all" reasonable steps to prevent harassment arising (not just "reasonable" steps). This was something that it also proposed in the run up to the election. Bearing this in mind, employers may want to ensure they work to this higher standard to set them in good stead ahead of this proposed change. We will keep you posted on developments.

CLICK HERE FOR SOURCE ARTICLE

UK Equal Pay Update

In a decision that could prove a significant milestone in the story of equal pay in the UK – an Employment Tribunal has decided that the retailer Next could not rely on "market forces" to justify differences in basic pay between the predominantly female retail consultants in Next stores and their (higher earning, and mostly male) warehouse operative colleagues. The claimants' solicitors have suggested that up to £30m may be payable in compensation to the retail consultants.

A previous Tribunal decision had found that these particular groups of Next employees were conducting work of equal value – so this decision related solely to whether the employer could rely on the "material factor defence" to justify the pay differential.

Next were able to establish the defence in relation to certain bonuses and other benefits, but when it came to the differential in basic pay, the employer could not make out the defence.

Next argued that it had a legitimate aim in paying a lower rate of basic pay (based on the market rate for such roles) to its retail consultants – namely shoring up its viability, resilience and successful business performance. But the Tribunal concluded that, when it came to the differential in basic pay, Next *could* have afforded to pay its retail staff more but instead prioritised keeping its labour costs in check – i.e. this was about costs saving (only) which is not a legitimate aim that can be relied upon to establish the defence.

The Employment Tribunals are alive to the issue that market rates for particular roles may be tainted by historical attitudes and perceptions about the value of *men's work* versus *women's work* – and that citing market forces will not of itself excuse the disparity between pay rates for roles that are predominantly held be men and those predominantly held by women. Employers who rely on this argument risk being criticised for perpetuating the kind of pay inequality that the legislation is intended to address.

This decision is the first in a string of similar cases expected to be heard in the Employment Tribunal in the coming months relating to the UK's largest supermarkets and other retailers, but it has potential ramifications for employers across all sectors.

It is a first instance decision (so not binding on other Tribunals) and Next have indicated they will appeal. But if the decision is not overturned, employers will find it increasingly difficult to base a defence to an equal pay claim on the fact that they simply "paid the going rate" for a particular type of job, and did so to maintain their profitability. The focus for justifying different rates of pay may well shift therefore towards other issues that extend beyond mere cost savings linked to the particular challenges facing the business at the relevant time.

Employers will be paying close attention to the progress of the similar claims against major supermarkets, and to Next's appeal in the coming months. This is a challenge for employers that may be compounded if the Labour government follows through with its plans to introduce an Equality (Race and Disability) Bill extending full equal pay rights to ethnic minority workers and disabled people.

CLICK HERE FOR SOURCE ARTICLE

New Brazil Pay Transparency Report Is Due by the End of September 2024

- Companies with more than 100 employees in Brazil must post their pay transparency report by September 30, 2024.
- This will be the second report since the law and its regulations went into effect earlier this year.
- Regulations to implement Brazil's law requiring the pay transparency report and action plan have been heavily criticized in the business community.
-

In July 2023, the Brazilian Congress passed a law[1] with new and more stringent rules relating to equal pay, with a particular focus on the gender pay gap. The law requires a number of measures be implemented to make compensation criteria more transparent, increase oversight by the labor authorities, promote diversity and inclusion, and create training and education for women on entering, remaining, and advancing in their careers on equal terms with men.

The regulations issued by the Ministry of Labor in November 2023[2] then focused on two aspects of the law: the mandatory pay transparency report for companies with more than 100 employees, which must be publicized twice a year, and the

"Action Plan" companies that showed a gap must implement.

Companies with more than 100 employees became particularly frustrated with the Ordinance[3] because the Ministry decided that the pay transparency report would be prepared by the Ministry, not the companies, with data it had collected through other mandatory reports made by such companies through the eSocial platform and additional information provided through a questionnaire issued by the Ministry. The shock was even bigger when the companies learned in February 2024 that they would not have full access to the criteria and data used by the Ministry to prepare the reports (except that the compensation used was from 2022) and saw that the basic questionnaire was multiple choice and did not allow the inclusion of any explanation for pay disparities.

In March 2024, companies received the reports from the Ministry of Labor, all of which showed a significant gap between men's and women's compensation. According to the Ministry of Labor, 49,587 companies in Brazil received the reports from the Ministry. The information of all such companies showed that women earn on average 19.4% less than men in the same "position." This data was likely flawed because the Ministry grouped positions based on the Brazilian Occupational Classification and did not account for a number of other variables such as seniority, experience, and performance, which companies generally consider when setting compensation.

The March 2024 data also showed that only 32.6% of the companies had a policy to incentivize the hiring of women and even fewer had policies specifically targeting certain groups: Black women (26.4%), women with disabilities (23.3%), members of the LGBTQ+ community (20.6%), women heads of household (22.4%) and women victims of violence (5.4%). Only 38.3% of companies had specific policies to promote women to positions of management.

Many companies that decided to publish their reports did so but included their own explanation about why they did not believe the numbers to be accurate and even posted some specific comparisons with their own numbers.

Based on the results and the potential backlash that an unclear report could cause to the companies' brand, some other companies either individually or through industry-wide organizations sought an injunction to avoid the obligation to publicize their reports, claiming that the regulations went beyond the scope of the law and citing possible damage to the companies' competition and freedom. The two most relevant cases were filed by the Federation of the Industries of the State of Minas Gerais (FIEMG) and the National Confederation of Industry (CNI).

FIEMG filed a public civil action[4] with the Federal Regional Tribunal of the 6th Region (TRF-6) in March to suspend the obligation of companies to publish the pay transparency report, which included a request for an urgent preliminary injunction. The injunction was granted, and while the Ministry of Labor was able to reverse the decision, on July 18, the FIEMG's appeal was successful, and the suspension reinstated. This decision applies to all companies in Brazil. We believe this decision may be vulnerable in protecting companies not represented by FIEMG, however, as there may be discussion as to the legitimacy of FIEMG representing companies not part of the organization, the competence of the Federal Court of the State of Minas Gerais to hand down a decision with national effects covering all companies, and the effective scope of the decision.

The other relevant lawsuit is the ADI 7.612, filed by CNI with the Brazilian Supreme Court on March 12, 2024, alleging the unconstitutionality of the law and its regulations. Justice Alexandre de Moraes was assigned as the rapporteur, and we are still waiting for the case to be included in the court's agenda for judgment.

Companies with more than 100 employees are now facing the same process and dilemma. The Ministry of Labor distributed a new questionnaire in the beginning of August for the companies to answer. The questionnaire was almost identical to the last version, except for adding a question on whether companies have a specific policy to promote the hiring of indigenous women. The ministry provided no further explanation or relevant information about the criteria or possible revision of the criteria or methodology companies believe to be flawed. This time, as of August 31, only 31,936 companies answered the questionnaire, out of the estimated 52,000 companies with more than 100 employees in Brazil. The companies that have more than 100 employees and are not covered by the legal injunction will have to post their new report by September 30, 2024, either on their websites or social media platforms, or may face some potentially steep fines.

Companies that do not comply with the requirement of posting their report may be fined up to 3% of their total payroll, limited to 100 monthly minimum wages (*i.e.*, R$142,200 or USD28,250), and those that require an Action Plan have 90

days to submit such plan from the date they receive the order.

It seems that the Ministry of Labor did not fine any company that did not post the first report on its website and have not ordered companies with a compensation gap to implement an Action Plan. However, the Ministry may not continue to be this lenient when the new report in September is due.

The Action Plan is still a vague idea. According to the law and regulations, the plan to mitigate the discrepancies must include targets, deadlines for achieving such targets, and mechanisms to measure the achievement of the targets, including an annual plan with the execution chronology. The plan must include the creation or development of programs to promote diversity and inclusion, and steps to engage, maintain, and promote women to higher management positions. The plan must be prepared with the participation of the applicable union and employees' representatives. The plan will then have to be filed with the union. Some companies have been working on an Action Plan since the last report was issued in March, but it is unclear whether their plans will work in reality, particularly with an extremely short deadline of 90 days to prepare them.

Brazil Pay Transparency Law Compared to the EU Directive and some U.S. State Laws

Although Brazil's efforts to reduce a gender pay gap is in line with the current global trend and ahead of other Latin America countries, its law and regulations seem to have been rushed and lack practicalities that other countries took into consideration when issuing their regulations. A good example is how the points raised above compare with the EU Directive.[5]

- The EU Directive issued by the European Parliament on May 10, 2023, will only have to be transposed by its member states by 2026, giving companies plenty of time to prepare and adjust to it.
- By June 2027, employers with 250 or more employees will have to provide a report on the gender pay gap and every year thereafter. Employers with 150 to 249 employees will have to issue a report by June 2027 and then only every three years and, by June 2031, employers with 100 to 149 employees will issue their report, and every three years thereafter.
- The report will be prepared by the companies using their own methodology, after consulting with workers' representatives.
- Companies required to report with a gap of 5% or more that cannot be justified and is not cured within six months from the date of the report's submission must conduct a joint pay assessment and put together a plan, in cooperation with their workers' representatives, to remedy such gap within a reasonable period of time.

Unlike the EU Directive and some U.S. state laws such as those in California, Colorado, and New York, the Brazil pay transparency law does not impose obligations to disclose initial pay or pay range to candidates or prohibit employers from asking candidates about their pay history. Under the EU Directive, job applicants have the right to receive from a prospective employer information about the initial pay or pay range and the employer cannot ask their pay history. As to the United States, a patchwork of state and local laws containing differing requirements and nuances on pay transparency are a whole other issue for multistate and multinational employers trying to come up with a formula to address pay disparities from a global perspective.

CLICK HERE FOR SOURCE ARTICLE

Brazil's Data Protection Authority Issues Rules Clarifying Data Transfers

Wondering what the requirements are for transferring personal information out of Brazil? Under the country's Data Protection Law, extra-territorial transfers of personal information are regulated in much the same way as in EU Member States. Parties can transfer personal information from Brazil to a third country only in limited circumstances. This includes, among other scenarios, if the entity receiving the information is located in a country that has been deemed adequate or if the parties put in place approved standard contractual clauses.

There have been questions for both of these, which were recently addressed through rulemaking by the Brazilian data protection authority:

- Adequacy: Currently, no country has been deemed adequate, although Brazil is working with the EU to establish that the EU's privacy laws meet the adequacy level. Similarly, the EU is working to recognize Brazil's law as adequate. Under the new rules, to make the process run more smoothly, the data protection authority (ANPD) has

set out the criteria to assess if another region's privacy law should be found adequate.
- Standard Contractual Clauses: Until there are adequacy decisions, those wishing to export personal data out of Brazil will need to rely on other measures. Those other measures include standard contractual clauses or SCCs. These were also addressed in the new rulemaking. The rules include a set of approved SCCs. In addition, the rules contemplate using SCCs that differ from the approved set. Companies who wish to rely on SCCs will have until August 2025 to put sufficient ones in place.

In addition to adequacy decisions and SCCs, the rules address other questions and issues that have arisen relating to cross-border transfers. This includes providing -upon a data subject's request- a copy of the contract that was relied on for making the transfer of information.

Putting It Into Practice: For those who wish to rely on SCCs for data transfers from Brazil, companies will have until August 2025 to put them in place. These might mirror SCCs being used for other jurisdictions, and we expect to see more clarification from the ANPD on this point. We also anticipate seeing more countries receiving "adequacy" decisions from Brazil in the near future.

CLICK HERE FOR SOURCE ARTICLE

The Significance of Background Checks and Due Diligence in Indian Corporate Dispute Cases

In India's corporate landscape, disputes involving individuals can stem from various issues such as contractual breaches, fraud, or competitive conflicts. Conducting rigorous background checks and thorough due diligence on the parties involved is crucial, providing critical and relevant information to substantiate legal cases. This article explores the significance of various components of background checks and due diligence in corporate dispute cases.

Open-Source Intelligence (OSINT)

Open-Source Intelligence (OSINT) involves the collection and analysis of publicly available information to aid in decision-making. In corporate disputes, OSINT can provide valuable insights into an individual's activities, reputation, and behaviour. This includes:
- Social Media Analysis: Monitoring social media platforms can reveal a lot about an individual's personal and professional interactions, opinions, and public perception. It can also uncover any negative publicity or potential red flags that might be relevant to the dispute.
- News and Media Reports: Articles and news reports can provide historical context and highlight any previous disputes or legal issues involving the individual.
- Public Records: Accessing public records such as property ownership, criminal records, and court records can provide a deeper understanding of an individual's legal standing and personal history.

Government Database Checks

Government databases are treasure troves of information that can be crucial in corporate disputes. These checks ensure that the information is legitimate and verified by authoritative sources. Key areas include:
- Regulatory Filings: Examination of corporate filings with regulatory authorities, including the Security and Exchange Board of India (SEBI) and Ministry of Corporate Affairs, to verify compliance and governance practices.
- Litigation History: Review of court records to identify any legal disputes or litigation involving the subject, indicating potential patterns of legal issues.

Financial Tracking

Financial tracking involves scrutinizing an individual's financial health and transactions to uncover any discrepancies or signs of misconduct. This includes:
- Credit Reports: Analysing credit reports can provide insights into an individual's financial stability and history of debt management practices.
- Transaction History: Reviewing transaction records can help identify any suspicious activities, such as unusual transfers or discrepancies in financial reporting.

- Asset Verification: Checking for the existence and ownership of significant assets can reveal hidden wealth or financial obligations.

Source Information

Incorporating source information into background checks ensures that all gathered data is credible and reliable. This involves:

- Verification of Sources: Cross-referencing information from multiple sources can help verify its accuracy and authenticity.
- Interviews and Expert Consultations: Speaking with colleagues, former employers, or other relevant individuals can provide additional context and firsthand insights into the individual's character and behaviour.
- Document Analysis: Examining contracts, agreements, and other legal documents can uncover critical details relevant to the dispute.

Conclusion

Background checks and due diligence are indispensable tools in corporate dispute cases, offering a comprehensive understanding of the individuals involved and helping to uncover potential risks, verify information, and support informed decision-making. The case example demonstrates the importance of these processes in identifying hidden risks, such as past credit defaults and questionable business practices, which could have jeopardized the investment. Additionally, it highlights how thorough due diligence can protect a client's reputation by proactively addressing potential reputational risks and ensuring compliance with legal and regulatory standards. These key takeaways underscore the critical role that background checks and due diligence play in fostering a culture of transparency and accountability in the corporate landscape.

CLICK HERE FOR SOURCE ARTICLE

Japan Criminalizes Cannabis With 7-Year Prison Sentence, Medical Marijuana Remains Legal

Japan is set to make a significant shift in its cannabis policy by criminalizing personal use while simultaneously legalizing medical products derived from the plant.

According to Kyodo News, the health ministry confirmed Thursday that these changes, aimed at regulating cannabis use and expanding access to cannabis-derived medicines, will take effect on December 12.

Japan Will Criminalize Cannabis Use

Although Japan has long banned the possession and cultivation of marijuana, the country had yet to penalize its use. This loophole was initially left to protect hemp farmers, who might inadvertently absorb trace amounts of cannabis compounds while cultivating the plant for industrial purposes.

However, growing concerns about drug abuse, particularly among young people, have prompted Japan to reverse its stance. Under the revised laws, using cannabis will be illegal, with violators facing up to seven years in prison. Authorities say this harsh stance will address the rise in drug misuse and serve as a deterrent. Japan's strict drug policies have long been known for their zero-tolerance approach, but this move marks a new era of control over even personal use.

Medical Marijuana

In contrast, Japan is opening the door to medical marijuana products. The revised laws will permit the use of cannabis-derived medicines, a significant step for patients who have been advocating for broader access to treatments.
While cannabis-based drugs have thus far been limited to clinical trials, the new legal framework will allow for their prescription and wider use in medical care.

Patient groups have been particularly vocal in pushing for cannabidiol (CBD) medicines, which are already approved in many parts of the world, including Europe and the United States.

These drugs are used to treat conditions like severe epilepsy. The legal change offers hope for patients who have struggled to find effective treatments under Japan's restrictive drug policies.

CLICK HERE FOR SOURCE ARTICLE

MISCELLANEOUS DEVELOPMENTS

Quebec's Anonymization Regulation: A Step-by-Step Guide For Businesses

As of May 30, 2024, organizations subject to Quebec laws must comply with the *Regulation respecting the anonymization of personal information* (French version here) ("Quebec Anonymization Regulation"). The main objective of this regulation is to provide a standardized framework for the anonymization of personal information.

This regulation is adopted in furtherance to Article 23 of the *Act respecting the protection of personal information in the private sector states* ("Quebec Privacy Act") and Article 73 of the *Act respecting Access to documents held by public bodies and the Protection of personal information* ("Access Act") requiring that "information anonymized (…) must be anonymized according to generally accepted best practices and according to the criteria and terms determined by regulation."

As such, under Quebec privacy laws, organizations must anonymize personal information in accordance with "generally accepted best practices" and "the criteria and terms determined by regulation." The Quebec legislator has therefore adopted the Quebec Anonymization Regulation, which sets out the criteria and terms it expects organizations to comply with.
In this article, we will provide you with an overview of the requirements set out in the Quebec Anonymization Regulation and a step-by-step guide for anonymizing personal information.

1. Requirements of the Quebec Anonymization Regulation

Under the Quebec Anonymization Regulation, personal information must be anonymized according to the criteria it sets out. Here is a summary of the requirements in a step-by-step format:

1.1. Step 1: Purpose Identification

Before starting the anonymization process, organizations must clearly establish the purpose for which they intend to use the anonymized information. In other words, companies must first identify why they need anonymized information. This ensures that organizations intend to use anonymized information for a legitimate purpose and can adequately apply appropriate anonymization techniques set out in the Quebec Anonymization Regulation.

It must be noted that if organizations wish to use their anonymized information for purposes other than those initially determined when the personal information was anonymized, they must ensure that the new purposes are consistent with the requirements of the Quebec Anonymization Regulation.

1.2. Step 2: Supervised Anonymization Process

The Quebec Anonymization Regulation requires that the anonymization process be supervised by a qualified person in the field. This requirement ensures that the appropriate anonymization technique is used, a proper re-identification risk assessment is performed, and the integrity of the entire anonymization process is maintained.

1.3. Step 3: Initial Data Preparation

At the beginning of the anonymization process, organizations must remove all personal information from their dataset. In other words, any information that could directly or indirectly identify a person must be removed from the dataset.

1.4. Step 4: Re-Identification Risk Analysis

Once the dataset is stripped of all personal information, organizations must ensure that individuals cannot be re-identified by performing a reidentification risk analysis, considering:

- the individualization criterion, the correlation criterion, and the inference criterion set out by the Quebec Anonymization Regulation; and,
- other reasonably available information, particularly in the public space, that could be used to identify a person

directly or indirectly.

1.5. Step 5: Anonymization Techniques and Security Measures

Based on the re-identification risks identified, organizations must establish and apply appropriate anonymization techniques consistent with generally accepted best practices. Additionally, organizations must implement reasonable data protection and security measures to reduce any identified re-identification risk.

1.6. Step 6: Post-Anonymization Risk Analysis

Once an organization has implemented appropriate anonymization techniques and security measures, it must conduct a new re-identification risk analysis. The results of this new assessment should demonstrate that, at all times (reasonably foreseeable in the circumstances):

- The anonymization process is irreversible; and,
- The anonymized information no longer allows the identification of a person, directly or indirectly.

Although the Quebec Anonymization Regulation does not require a result where there is zero risk of re-identification, it does state that the "residual risks of re-identification" be "very low" considering the following parameters:

- The purpose of the anonymization;
- The nature of the information;
- The individualization, correlation, and inference criteria;
- The risks posed by other available information, particularly in the public space; and,
- The efforts and resources required to re-identify the personal information.

1.7. Step 6: Ongoing Assessment

Organizations must periodically reassess their anonymized information to ensure it remains anonymized over time. This includes updating re-identification risk analyses already performed and considering technological advancements that could increase the risk of reidentification.

Any periodic assessment must continue to demonstrate that the anonymization process remains irreversible and that the anonymized information cannot be used to re-identify an individual. The Quebec Anonymization Regulation states that organizations should determine the appropriate reassessment interval based on the residual risks of re-identification identified during their re-identification risk analysis.

1.8. Step 7: Record-Keeping Requirement

Effective January 1, 2025, organizations must maintain a register documenting:

- a description of the anonymized personal information;
- the purposes for which the anonymized information will be used;
- the anonymization techniques and security measures applied; and,
- the date the re-identification risk analysis was performed, along with any updates.

2. Understanding the Anonymization Criteria

The Quebec Anonymization Regulation specifically identifies three anonymization criteria, namely:

- correlation criterion;
- individualization criterion; and
- inference criterion.

2.1. Correlation Criterion

The Quebec Anonymization Act defines the correlation criterion as "the inability to connect datasets concerning the same person." This criterion ensures that, once personal information has been anonymized, it is no longer possible to link different datasets that pertain to the same individual. In practice, organizations with multiple datasets should not cross-reference them

to re-identify an individual. In other words, this criterion prevents the reidentification of an individual through the combination of information from different sources.

2.2. Individualization Criterion

The Quebec Anonymization Act defines the individualization criterion as "the inability to isolate or distinguish a person within a dataset." The individualization criterion is designed to prevent any person from being singled out or distinguished within a dataset. Although a dataset may only contain anonymized information, it should be generalized enough so that no specific individual can be isolated from the rest of the dataset. This prevents scenarios where an individual's identity could be inferred by identifying unique characteristics or patterns within the same dataset.

2.3. Inference Criterion

The Quebec Anonymization Act defines the inference criterion as "the inability to infer personal information from other available information." The inference criterion focuses on preventing the deduction of a person's identity from anonymized information by analyzing it in conjunction with other available information. Although a particular dataset may not allow the identification of any person, this criterion ensures that it is not possible to infer personal information by piecing together information from other sources, such as the public space. The objective of this criterion is to have organizations assess the possible risk of re-identification based on the possible inference from information reasonably available from other sources allowing an individual to be identified.

A. European Influence on Quebec's Anonymization Criteria
The Quebec Anonymization Regulation is largely inspired by European developments over the years. More specifically, Opinion 5/2014 on Anonymisation Techniques by the Article 29 Data Protection Working Party represents a great source for the possible interpretation of the Quebec Anonymization Regulation in Quebec. This opinion outlines the limitations and effectiveness of various anonymization methods, emphasizing the risks of re-identification. The key European anonymization criteria they present align closely with Quebec's regulation:

1. Singling Out (similar to the Individualization Criterion in Quebec): Ensuring that individual records cannot be singled out within a dataset;
2. Linkability (similar to the Correlation Criterion in Quebec): Preventing the linkage of records across different datasets to a single individual; and
3. Inference (the same as the Inference Criterion in Quebec): Reducing the likelihood of inferring personal information from anonymized data.

3. Conclusion

Quebec's Anonymization Regulation represents a significant step forward in ensuring that personal information is protected in a way that aligns with global privacy standards. Organizations can effectively minimize the risk of re-identification by adhering to the defined anonymization criteria and processes outlined in the Quebec Anonymization Regulation. The Quebec Anonymization Regulation not only provides a roadmap for compliance but also encourages organizations to adopt best practices in data management. Organizations must remain proactive, continually assess their anonymization needs and methods, and ensure compliance with Quebec privacy law requirements.

CLICK HERE FOR SOURCE ARTICLE

Politics in the Workplace and the Risks of Social Media

In 2017, former Supreme Court Justice Anthony Kennedy noted in *Packingham v. North Carolina*[1] that the most important place for the exchange of ideas is no longer the physical town square but cyberspace and, in particular, social media. Social media has only gained currency since then as the predominant forum for political discourse.

As election season enters its final stretch and international events such as the Israeli-Palestinian conflict are dominating the headlines, employers should expect that many of their employees will engage with political content on social media. Although political engagement by the citizenry is necessary for a democracy to thrive, the transformation of social media into a digital town square also generates issues in the areas of employment and labor law, with significant implications for

employers. As a result, employers must be attuned to these risks and prepared to negotiate the line between employees' rights and the limits on those rights, to prevent and address any employment-related issues that may arise.

Risks of Employee Use of Social Media for Political Purposes

1. Social Media Exacerbates the Drawbacks of Political Discourse in the Workplace.

Because they involve subjects of personal significance to employees, political discussions in the workplace are often problematic, and even minor disagreements can turn heated. Polling data reveal that many find political discussions stressful and frustrating, rather than informative or interesting, and a majority think that another's political views "say a lot" about their character, a statistic that suggests political disagreement can erode characteristics of high-performing teams, including mutual trust, collaboration, and communication.[2] This raises a concern that political discussions might negatively affect productivity, employee morale and relationships among coworkers.

While political discourse in the workplace has always been fraught, social media tends to exacerbate its downsides. As the U.S. Court of Appeals for the Ninth Circuit recently explained in a sexual harassment case, *Okonowsky v. Garland*, social media differs from traditional means of communication in important ways. Unlike offhand comments shared among a small group in a breakroom, "[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."[3] Other users can amplify a post by "liking" or "supporting" it, leaving a comment, or reposting it to their own account—features which, in tandem with proprietary algorithms, allow a fraction of content to go "viral." Even with non-viral content, social media offers users a much wider audience than they would otherwise likely have. Given these features, employee use of social media to engage in political speech could have an outsized detrimental effect on workplace relationships and culture.

2. Social Media Increases Public Relations Dangers for Employers.

Because of social media's extensive reach, a company's consumer base may come to associate employers with content created and shared on social media by their employees. It is often easy to discover where the owner of a certain social media account works through a simple online search, if the information is not contained in the individual's profile itself. Should an employee's social media post be politically offensive or controversial, and the employee is readily connected to a particular business, consequent exposure may generate complaints from coworker or the consumer public. In extreme cases, such exposure could even threaten damage to the company's brand.

3. Social Media Use Could Expose Employers to Discrimination and Harassment Claims.

In July, the Ninth Circuit overturned a district court decision finding no actionable harassment where the conduct occurred entirely outside of the workplace. *Okonowsky v. Garland* involved a supervisor's personal Instagram account that contained "overtly sexist, racist, anti-Semitic, homophobic, and transphobic memes." The Ninth Circuit rejected the employer's position that social media generated outside the workplace cannot form the basis of a hostile work environment claim. The court pointed out that coworkers could view, comment on, and otherwise interact with the offensive posts inside and outside the workplace. "[I]n 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 rejected the distinction between conduct occurring in the workplace and social media content produced and viewed outside of work.

Okonowsky highlights the risk that employees' entirely offsite use of social media could contribute to a hostile work environment if the content is harassing and affects the working environment. Further, because the standard for hostile work environment accounts for the totality of circumstances, social media posts need not target the plaintiff to subject an employer to liability. The Ninth Circuit's position is consistent with Equal Employment Opportunity Commission (EEOC) enforcement guidance released in April, which indicates that conduct on social media platforms outside the workplace may contribute to a hostile work environment. Notably, however, the EEOC indicated that social media content will not generally, by itself, lead to a hostile work environment unless the content targets the employer or its employees.

The Israeli-Palestinian conflict has brought related issues to the forefront. The October 7, 2023 Hamas attack and Israel's response have prompted an outpouring of strong reactions on social media. Because the conflict entails issues of ethnicity, religion, and national origin, employers that act against employees for their public statements about the conflict risk an anti-

discrimination lawsuit. Over the past year, many businesses have faced scrutiny for allegedly disciplining and discharging employees who were outspoken in their support of either Israel or Palestine, and some are now defending lawsuits brought by employees who were sanctioned for this conduct.

4. Social Media Posts Can Be Used as Evidence of Bias.

Political content on social media frequently touches upon hot-button issues such as reproductive rights, immigration, LGBTQ rights, and affirmative action and other efforts at increasing diversity. Because these political issues are entwined with characteristics protected by anti-discrimination law, if a manager or another in a decision-making role discusses controversial topics on social media, a litigant could use the decision-maker's statements as circumstantial evidence of bias, as courts have recognized.

Even less-controversial statements may pose risks. Consider, for example, a manager who advocates on social media for younger political leadership. (A significant majority of Americans, regardless of party affiliation, supports age limits for Congress and the Supreme Court.[4]) Because social media searches are a common litigation tool, even if the manager has a limited social media following, these posts are unlikely to be overlooked. And even if not inflammatory, they could become an exhibit in an age bias lawsuit after the same manager oversees a round of layoffs.

Limits on Employers' Ability to Curtail Employee Social Media Use for Political Purposes

Because of the risks noted above, employers may at first blush wish to monitor and restrict employee social media usage, including outside of work. While the First Amendment does not restrict private employers from policing their employees' speech, other legal and social commitments may. Practically speaking, because of a robust "free speech" culture in the United States, a prevailing notion that persons should be able to express themselves authentically, and the growing expectation that professionals build an online "brand," employers may shy away from regulating their employees' speech on social media, despite countervailing risks.

There are also legal limits on actions employers can take in response to employee social media engagement. Some states, like California and Colorado, prevent employers from terminating employees for their lawful off-duty conduct, while others, like South Carolina and Louisiana, protect employees from discharge for their political opinions. California and New York, among other states, forbid employers from preventing employees from engaging or participating in politics. In notably broad fashion, Connecticut protects employees from discipline for the exercise of their First Amendment rights.[5]

Moreover, dozens of states have social media privacy laws that prohibit employers from accessing an employee's non-public social media posts. An employer intending to discipline an employee for social media post must be able to prove they did not obtain the post in violation of the applicable law's privacy safeguards. Under these laws, any discipline issued as a result of improperly obtained social media posts could subject the employer to liability. Given the various ways states address these issues, employers must carefully review state and local laws to ensure their remedial efforts are consistent with these frameworks.

Another limiting consideration for employers that seek to regulate employees' political speech on social media is the National Labor Relations Act (NLRA). The NLRA, which applies to all non-supervisory employees, both unionized and non-unionized, guarantees employees "the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and *to engage in other concerted activities for* the purpose of collective bargaining or *other mutual aid or protection*," as well as the right "to refrain from any or all such activities," more simply known as "protected concerted activity."[6] [Emphasis added.] The National Labor Relations Board (NLRB), the federal agency that enforces the NLRA, provides guidance on its website explaining that "[u]sing social media can be a form of protected concerted activity" but is limited to "the right to address work-related issues and share information about pay, benefits, and working conditions with coworkers on Facebook, YouTube, and other social media."[7] The NLRB's guidance further recognizes certain limitations on how the NLRA applies to social media postings:

But just individually griping about some aspect of work is not 'concerted activity': what you say must have some relation to group action, or seek to initiate, induce, or prepare for group action, or bring a group complaint to the attention of management. Such activity is not protected if you say things about your employer that are egregiously offensive or knowingly and deliberately false, or if you publicly disparage your employer's products or services without relating your

complaints to any labor controversy.[8]

As one might expect, the work-relatedness of employees' socio-political speech has been the subject of litigation. As far back as 1978, the Supreme Court made clear that employees' support for employees other than their own employer's can be protected concerted activity, but "at some point the relationship becomes so attenuated that an activity cannot fairly be deemed to come within the 'mutual aid or protection' clause."[9] The NLRB under the present administration has dramatically expanded the concept of protected concerted activity. Recent NLRB decisions suggest that individual employee speech directed at political or social causes *could* trigger NLRA protection, but not all such speech is connected to work-related concerns. While these cases did not involve social media, the NLRB's reasoning would apply to activity on social media.

Recommended Practices

- **Social Media Policies.** Employers should consider developing a clear policy that establishes acceptable contours for employee use of social media, including online political engagement. The policy should specify which types of political activity or expressions are regulated and clarify whether it applies to personal use of social media or only when social media is used during working time and on company resources. Further, any restrictions must advance a legitimate and substantial business interest, such as preventing unlawful workplace discrimination and harassment. In crafting a social media policy, employers must account for activities and communications protected by the NLRA and applicable state and local laws. Because of the stringent standards for workplace policies and rules adopted by the NLRB in *Stericycle, Inc.*,[10] employers should consult with experienced labor counsel to ensure their policies are not subject to the challenge under the NLRA.
- **Communication Regarding Policies.** As the election season progresses, employers should remind employees about their social media and related policies. Before doing so, employers should review their current policies to ensure they align with the latest legal developments.
- **Consistent Application of Policies and Investigations.** Employers should enforce all policies and rules in a consistent, uniform, and non-discriminatory manner. If an investigation is necessary, the investigation must be conducted thoroughly and impartially. In conducting the investigation, employers should be mindful of laws that prohibit employers from forcing employees to allow access to their social media accounts. If a company can demonstrate that it has applied its social media policy in an equitable manner, and has conducted an impartial investigation before taking any adverse action, it will have a stronger defense against discrimination claims.
- **Training.** Employers should train employees on their social media policy, and should also consider training supervisors and managers on how to address complaints involving an employee's social media communication.
- **State and local laws.** As detailed above, some states offer more robust employee protections in this domain than does federal law. Before implementing a social media policy or investigating an employee's social media use, employers must understand the scope of protection offered by the particular jurisdictions in which they operate.[11]

CLICK HERE FOR SOURCE ARTICLE

What Responsibilities Do Employers Have Under New York State's Retail Worker Safety Act?

New York Governor Kathy Hochul signed the Retail Worker Safety Act (S. 8358B/A. 8947C) into law on Sept. 4, 2024. The Act will require covered retail employers to:

1. Adopt a retail workplace violence prevention policy (effective date of on or about March 3, 2025);
2. Develop and implement training programs to prevent workplace violence (effective date of on or about March 3, 2025); and
3. Install panic buttons at the workplace (effective date of on or about Jan. 1, 2027).

Covered Employers

Covered employers for the policy and training requirements include any person, entity, business, corporation, partnership, limited liability company, or association employing at least 10 retail employees.
Covered employers for the panic button requirements are entities that employ at least 500 retail employees nationwide.
Retail employees are employees working in a retail store. A retail store is defined as a store that sells consumer commodities at retail and is not primarily engaged in the sale of food for consumption on premises.

Violence Prevention Policy

Seeking to ensure retail employees are prepared for workplace violence incidents, the Act requires employers to adopt and disseminate, both at hire and annually, a retail workplace violence prevention policy as part of the mandated training. The New York State Department of Labor will create and publish a model retail workplace violence prevention guidance document and retail workplace violence prevention policy for each covered employer to use in developing its own policy.

The model policy will list factors that may put retail employees at risk of workplace violence, including, but not limited to:

- Working late night or early morning hours;
- Exchanging money with the public;
- Working alone or in small numbers; and
- Permitting uncontrolled access to the workplace.

The model policy also will:

- Set out methods employers can use to prevent workplace violence, such as establishing and implementing reporting systems for incidents of workplace violence;
- Include information concerning federal, state, and local statutory provisions available to victims; and
- Clearly provide that retaliation against individuals who complain of workplace violence, raise situations in the workplace that could put retail employees at risk, or testify or assist in any proceeding under the law is unlawful.

Workplace Training Program

The Act directs the New York State Department of Labor to produce a model workplace training program and requires covered employers to provide such training. The interactive training program will include, but not be limited to:

- Examples of measures retail employees can use to protect themselves when faced with workplace violence from customers or coworkers;
- De-escalation tactics;
- Active shooter drills;
- Emergency procedures; and
- Instruction on the use of security alarms, panic buttons, and other related emergency devices.

The Act requires the Department's model program to include information addressing conduct by supervisors and any additional responsibilities for supervisors, including ways to address workplace emergency procedures and training on areas of previous security problems. As part of this training, covered employers must communicate to all retail employees a site-specific list of emergency exits and meeting places in case of emergency.

The workplace violence prevention training must be provided to all retail employees upon hire and on an annual basis thereafter. In addition to disseminating the policy, employers must disseminate the training program.

Panic Button

Employers subject to this requirement must provide access to panic buttons throughout the workplace or provide all retail employees with wearable or mobile phone-based panic buttons (if the second option is used, such buttons cannot be used to track employee locations except when the panic button is triggered). The panic buttons must immediately contact the local 911 public safety answering point (PSAP) when pressed. Further, the panic button must provide the PSAP with information pertaining to the employee's location and dispatch local law enforcement to the workplace.

Takeaways for New York Employers

Covered employers should ensure compliance with the Act. The New York Department of Labor will be issuing its model retail workplace violence prevention policy template and model training program. Compliance guidance is also expected. The model retail workplace violence prevention policy and related information will be publicly available and posted on the Department's website.

CLICK HERE FOR SOURCE ARTICLE