APRIL 2025

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 and involves following the rules and regulations set forth by the Fair Credit Reporting Act (FCRA) and local ordinances.

CLICK FOR PAST UPDATES

TABLE OF CONTENTS

SCREENING COMPLIANCE UPDATE | APRIL 2025

This monthly publication is intended to bring to your attention screening industry related articles written by subject matter experts and published online to assist you with establishing and keeping a compliant background screening program.

PLEASE NOTE: Spellings of words in International articles such as those written in the British English format are native to the original author and differ from the spellings of words in the American English format.

EXECUTIVE SUMMARY

April 2025 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: The U.S. Citizenship and Immigration Services (USCIS) published an updated version of the Form I-9. The revised Form I-9 has an edition date of 1/20/2025 and an expiration date of 5/31/2027. The updated Form I-9 is already available on the USCIS website.
- STATE DEVELOPMENTS: In February 2025, fifteen State Attorneys General issued written guidance entitled "Multi-State Guidance Concerning Diversity, Equity, Inclusion, and Accessibility Employment Initiatives" in response to concerns from the private sector about DEI or DEIA initiatives following President Donald Trump's Executive Orders that direct federal agencies to aggressively pursue "illegal DEI" programs.
- INTERNATIONAL DEVELOPMENTS: Several Member States of the European Union (EU) have issued draft legislation for a "Pay Transparency Directive" that will take the necessary measures to ensure that "employers have pay structures ensuring equal pay for equal work or work of equal value."

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 into 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

President Trump Issues Executive Order Aimed at Eliminating Disparate Impact Liability Under Anti-Discrimination Laws

On April 23, 2025, the White House issued an Executive Order ("EO") entitled "Restoring Equality of Opportunity and Meritocracy," which aims to "eliminate the use of disparate-impact liability in all contexts to the maximum degree possible." First recognized under Title VII of the Civil Rights Act of 1964 ("Title VII") by the U.S. Supreme Court in *Griggs v. Duke Power Co.* (1971), disparate impact liability provides that a policy or practice that is facially neutral and applied without discriminatory intent may nevertheless give rise to a claim of discrimination if it has an adverse effect on a protected class, such as a particular race or gender. Disparate impact liability has also been recognized under fair housing laws and in other contexts.

The EO characterizes disparate impact liability as creating "a near insurmountable presumption of unlawful discrimination . . . where there are any differences in outcomes in certain circumstances among different races, sexes, or similar groups, even if there is no facially discriminatory policy or practice or discriminatory intent involved, and even if everyone has an equal opportunity to succeed." The EO further states that disparate impact liability "all but requires individuals and businesses to consider race and engage in racial balancing to avoid potentially crippling legal liability" and "is wholly inconsistent with the Constitution."

To that end, the EO, among other things:

- directs all executive departments and agencies to "deprioritize enforcement of all statutes and regulations to the extent they include disparate-impact liability," including but not limited to Title VII;
- orders the Attorney General, within 30 days of the EO, to report to the President "(i) all existing regulations, guidance, rules, or orders that impose disparate-impact liability or similar requirements, and detail agency steps for their amendment or repeal, as appropriate under applicable law; and (ii) other laws or decisions, including at the State level, that impose disparate-impact liability and any appropriate measures to address any constitutional or other legal infirmities";
- orders the Attorney General and the Chair of the EEOC, within 45 days, to "assess all pending investigations, civil suits, or positions taken in ongoing matters under every Federal civil rights law within their respective jurisdictions . . . that rely on a theory of disparate-impact liability, and [] take appropriate action" consistent with the EO;
- orders all agencies, within 90 days, to "evaluate existing consent judgments and permanent injunctions that rely on theories of disparate-impact liability and take appropriate action" consistent with the EO;
- orders the Attorney General, in coordination with other agencies, to "determine whether any Federal authorities preempt State laws, regulations, policies, or practices that impose disparate-impact liability based on a federally protected characteristic such as race, sex, or age, or whether such laws, regulations, policies, or practices have constitutional infirmities that warrant Federal action, and [] take appropriate measures" consistent with the EO; and
- orders the Attorney General to initiate action to repeal or amend regulations contemplating disparate impact liability under Title VI of the Civil Rights Act of 1964, which prohibits race, color, and national origin discrimination in programs and activities receiving federal financial assistance.

The EO also orders the Attorney General and the Chair of the EEOC to "jointly formulate and issue guidance or technical assistance to employers regarding appropriate methods to promote equal access to employment regardless of whether an applicant has a college education, where appropriate."

Takeaways

This EO is the latest evidence of shifting enforcement priorities by the federal agencies tasked with enforcing civil rights laws, including the EEOC. The ultimate scope of the EO's impact remains to be seen, particularly as it relates to the potential for preemption of disparate impact liability under state or local anti-discrimination laws. Congress has the authority to amend any federal statutes to specifically address a disparate impact theory of liability, and the courts will continue to have the ultimate say on whether and to what extent such a theory is cognizable under particular statutes. We anticipate further updates in this area and will continue to monitor and report on these updates.

Source: Lexology - Proskauer Rose- Allan Bloom, Elise M Bloom, Laura Fant and Rachel S Fischer

I-9 Alert! New Form I-9

Today, U.S. Citizenship and Immigration Services published an updated version of the Form I-9. The revised Form I-9 has an **edition date of 1/20/2025** and an expiration date of 5/31/2027. The updated Form I-9 is already available on the USCIS website.

Timing Considerations:

While multiple previous editions of Form I-9 remain valid until their respective expiration dates, as a matter of best practice, employers should begin using the new Form I-9 immediately to avoid any future errors. The edition date is located at the bottom left corner of Form I-9; the expiration date is located at the upper-right corner of Form I-9.

- Form I-9 (8/1/2023 edition) remains valid until its expiration date, 5/31/2027
- Form I-9 (8/1/2023 edition) remains valid until its expiration date, 7/31/2026 (**employers using this Form I-9 must update their electronic systems with the 5/31/2027 expiration date by July 31, 2026)

Updates to Form I-9:

USCIS made several changes to Form I-9:

- Renaming the fourth checkbox in Section 1 to "An alien authorized to work"
- Revising the descriptions of two List B documents in the List of Acceptable Documents (Driver's license or ID card) by removing the word 'gender' and replacing it with the word 'sex.'

Source: *Lexology - Fox Rothschild*

STATE, CITY, COUNTY, AND MUNICIPAL DEVELOPMENTS

New Mexico Is a Step Closer to Legalizing the Supervised Use of Psilocybin

We've previously highlighted psilocybin as an alternative treatment for various neuropsychiatric disorders, including anxiety, depression, and PTSD, along with legislative efforts at the state and federal levels to legalize and regulate the psychedelic drug. On March 12, 2025, New Mexico advanced its initiative to establish a therapeutic psilocybin program in the state.

By a bipartisan vote of 33-4, the New Mexico Senate passed Senate Bill 219, also known as the Medical Psilocybin Act, which now awaits a vote in the House of Representatives. If enacted, the bill would allow physicians to prescribe psilocybin to patients suffering from specific qualifying conditions such as major treatment-resistant depression, PTSD, substance use disorders, end-of-life care, and other conditions approved by the state's Department of Health.

The bill defines psilocybin as "the naturally occurring psychedelic compound 4-phosphoryloxy-N,N-dimethyltryptamine, also known as 4-PO-DMT, and its pharmacologically active metabolite psilocin, 4-hydroxy-N,Ndimethyltryptamine, found in certain mushrooms, but does not include synthetic or synthetic analogs of psilocybin". The bill proposes the establishment of a nine-member medical psilocybin advisory board to, among other things, "review and recommend to the [health] department for approval medical conditions that may benefit from the medical use of psilocybin" and "recommend formulation or preparation rules and dosage standards for psilocybin". If the bill is enacted, New Mexico would join Oregon and Colorado as the only states to legalize the supervised use of psilocybin.

Source: *Lexology - Womble Bond Dickinson (US) LLP – Al Windham and Madeline Campbell*

Massachusetts and Connecticut Join Other States in Issuing Guidance for Businesses on Diversity, Equity, Inclusion, and Accessibility Initiatives in the Workplace

On February 13, 2025, fifteen State Attorneys General issued written guidance entitled "Multi-State Guidance Concerning Diversity, Equity, Inclusion, and Accessibility Employment Initiatives" (the Massachusetts "Guidance" can be viewed here). The Guidance opens as follows:

The Attorneys General of Massachusetts, Illinois, Arizona, California, Connecticut, Delaware, Hawaii, Maine, Maryland, Minnesota, Nevada, New Jersey, New York, Oregon, Rhode Island, and Vermont are issuing this Guidance to help businesses, nonprofits, and other organizations operating in our respective states understand the continued viability and important role of diversity, equity, inclusion, and accessibility efforts (sometimes referred to as "DEI" or "DEIA" initiatives) in creating and maintaining legally compliant and thriving workplaces.

The Guidance was issued in response to concerns from many in the private sector about DEI or DEIA initiatives following President Trump's Executive Orders that (1) rescind affirmative action requirements in government contracting, and (2) direct federal agencies to aggressively pursue "illegal DEI" programs and policies of both government contractors and private employers. The Guidance aims to clarify the legality and utility of such programs for businesses, nonprofits, and other organizations operating in those fifteen states.

What Is DEIA and How Does it Differ from Affirmative Action?

Before we get into the Guidance, let's discuss how DEIA and affirmative action overlap and differ. DEIA and affirmative action share the goal of promoting diversity in the workplace. Affirmative action is intended to compensate for past discriminatory practices, such as against racial minorities and women, and is often implemented by establishing quotas or preferences in hiring and college admissions, among other areas. Critics of affirmative action claim that the practice is discriminatory and results in less qualified or unqualified employees and college admittees. Affirmative action has been found to be illegal except in limited circumstances. In a landmark 2023 decision, the U.S. Supreme Court struck down affirmative action programs that explicitly considered race as a factor in individual college admissions decisions. By a vote of 6-3, the Justices ruled that the admissions programs used by the University of North Carolina and Harvard College violated the Constitution's equal protection clause, which bars racial discrimination by government entities. We wrote about that decision here, and forecast that workplace DEIA initiatives might soon come under scrutiny.

While affirmative action is intended to give preference to groups that traditionally have been discriminated against, DEIA is a broader approach to creating an environment where everyone is treated equally, valued, and respected. DEIA can include educational programs, training, mentorship opportunities, and policy changes that are designed to promote inclusivity and equality. Unlike affirmative action, DEIA initiatives do not involve providing preferences to individuals based on protected characteristics, such as race or sex, in individual hiring or other employment decisions. Instead, according to the Guidance, DEIA initiatives ensure that employers can recruit, hire, and retain the most qualified employees, and that they do not overlook or bypass anyone because of a protected characteristic. According to the Guidance, well-designed DEIA initiatives also ensure that "the workplace provides the support needed for employees to continue to develop their skills and contribute to the success of their organizations" and "call on employers to pay attention to the (intentional and unintentional) impact their policies and practices have on different groups of current and prospective employees." DEIA is not designed to provide minorities with more opportunities than non-minorities but, rather, to afford comparable individuals with equal opportunities.

The EEOC and DOJ Weigh In

On March 19, 2025, the U.S. Equal Employment Opportunity Commission (EEOC) and the U.S. Department of Justice (DOJ) issued two technical assistance documents (found at: https://www.eeoc.gov/wysk/what-you-should-know-about-dei-related-discrimination-work; and https://www.eeoc.gov/what-do-if-you-experience-discrimination-related-dei-work). As noted in the introduction of the EEOC's "What to Do If You Experience Discrimination Related to DEI at Work," "[d]iversity, equity and inclusion (DEI) is a broad term that is not defined in Title VII of the Civil Rights Act of 1964…Under Title VII, DEI initiatives, policies, programs, or practices may be unlawful if they involve an employer or other covered entity taking an employment action motivated – in whole or in part – by an employee's or applicant's race, sex, or other protected characteristic." The DOJ's "What You Should Know About DEI-Related Discrimination at Work" materials similarly hold DEI against the lens of Title VII, which remains unchanged by the DEI Executive Orders issued and prohibits discrimination.

DEIA is Not Unlawful

Noting that the DEI Executive Order states what is already the law – that discrimination is illegal – the Attorney Generals' Guidance then criticizes it for conflating affirmative action with DEIA best practices. In doing so, the Guidance highlights the very important distinction that employers need to understand in today's climate: DEIA initiatives are not the same as affirmative action.

The Guidance emphasizes that DEIA initiatives are not illegal and questions the President's power to issue the DEI Order. In fact, the Guidance opines conclusively that the federal government *does not* have the legal authority to issue the DEI Order as it "prohibits otherwise lawful activities in the private sector or mandates the wholesale removal of [DEIA] policies and practices within private organizations, including those that receive federal contracts and grants."

The Guidance also sets forth some helpful best practices for effective DEIA initiatives with respect to recruitment and hiring, professional development and retention, and assessment and integration to ensure a diverse workforce.

The end of the Guidance includes a statement of commitment by the State Attorneys General to "stand ready to support organizations in our respective states as they continue to build and sustain successful and inclusive workplaces by implementing robust [DEIA] policies consistent with their obligations under our laws."

On March 4, 2025, the same coalition of Attorneys General issued a similar guidance to ensure K-12 schools, colleges, and universities across the nation understand the legality, viability, and importance of DEIA policies and practices in education. The Guidance is not wholly inconsistent with the EEOC and DOJ's technical assistance documents, but it definitely takes a different approach to the topic. Both continue to advise employers of their obligations under Title VII and employee and/or applicant's rights if they feel that they have suffered as the result of discrimination. The FAQs outlined by the EEOC advise of the process of seeking relief from any alleged discrimination through the filing of a complaint with the EEOC and/or equivalent state agencies, a process which remains unchanged.

What Should Employers Do Now?

Preferences in hiring are not the same as best practices for promoting diversity, equity, inclusion, and accessibility in the workplace. Because the current administration has been using the terms DEI and affirmative action interchangeably, we

recommend employers review the Guidance before eliminating or substantially changing any DEI initiatives to make sure that they have a clear understanding of what constitutes a DEI initiative vs. affirmative action.

Source: *Lexology - By Meaghan Murphy and Maureen James - Skoler Abbott P.C.*

Washington's Amended Fair Chance Act Will Impose Additional Obligations on Covered Employers

- Effective July 1, 2026, Washington's Fair Chance Act will further restrict the use of criminal records by covered employers.
- Covered employers face increased penalties after the law takes effect.

Washington State has an existing fair chance law, but the statute, as amended by HB 1747, will impose additional obligations on employers that consider criminal records when vetting job applicants or employees. The amended statute takes effect for most employers in July 2026 and so employers should plan to update their criminal record screening policies and standard forms of notice.

Expanded Prohibitions on Covered Employers
The amended statute will make the following actions unlawful:

- Inquiring about criminal records before first extending a conditional job offer.
- Taking a tangible adverse employment action based on an applicant's or employee's arrest record (excluding an adult arrest in which an individual is out on bail or released on their own personal recognizance pending trial) or juvenile conviction record.
- Taking a tangible adverse employment action based on an applicant's or employee's adult conviction record, unless the employer has a legitimate business reason for taking such action.

Expanded Obligations for Covered Employers
Employers must provide a form of pre-adverse action notice to the applicant or employee before taking a tangible adverse employment action. The notice must inform the applicant or employee of the record on which the employer is relying for purposes of assessing its legitimate business reason. The employer must hold open the position for a minimum of two business days to provide the applicant or employee a reasonable opportunity to correct or explain the record or provide information on the applicant's or employee's rehabilitation, good conduct, work experience, education, and training.

Employers also must provide a form of adverse action notice if they decide to take the tangible adverse employment action. Specifically, employers must provide such individuals with a written decision, including specific documentation as to the employer's reasoning and assessment of each of the relevant statutory factors, including the impact of the conviction on the position or business operations, and the employer's consideration of the applicant's or employee's rehabilitation, good conduct, work experience, education, and training.

Increased Penalties
The amendment increases the amount of the potential penalties for the first, second, and subsequent violations. The amendment also confirms that any penalties must be imposed per aggrieved job applicant or employee, for each violation.

Recommendations
Employers with operations in Washington should evaluate necessary changes in when and how they inquire into criminal history during the hiring process. They should also consider whether to undertake a broader (and privileged) assessment to strengthen their compliance with federal, state, and local employment laws that regulate use of a candidate's criminal history (including in Seattle). Suggested action items for employers with employees in Washington and other jurisdictions with fair chance hiring laws are as follows:

- Review and update job applications and related forms for impermissible inquiries regarding criminal records;
- Review and update workplace postings to help ensure all required postings are included;
- Review and update company webpages for necessary additions about fair chance hiring;
- Provide training to recruiters and other personnel involved in posting job openings;
- Provide training to personnel who conduct job interviews and make or influence hiring and staffing decisions to explain permissible inquiries into, and uses of, criminal history;
- Provide training to personnel involved in ordering and adjudicating background reports;

- Review written and electronic communications about the hiring process, including conditional job offer templates and pre-adverse action and adverse action notices; and
- Review the hiring and screening process to help ensure compliance, including the timing of background checks, the distribution of mandatory notices, and the application of mandatory deferral periods.

Source: *Lexology - Littler Mendelson PC- Rod M. Fliegel and Chad Joseph Kaldor*

COURT CASES

NetChoice Sues to Halt Louisiana Age Verification and Personalized Ad Law

On March 18, 2025, NetChoice filed a lawsuit seeking to enjoin a Louisiana law, the Secure Online Child Interaction and Age Limitation Act (S.B. 162) ("Act"), from taking effect this July. The Act requires social media companies subject to the law to obtain express consent from parents or guardians for minors under the age of 16 to create social media accounts. The Act also requires social media companies subject to the law to "make commercially reasonable efforts to verify the age of Louisiana account holders" to determine if a user is likely to be a minor. Further, the Act prohibits the use of targeted advertising to children.

In its complaint, NetChoice has raised a First Amendment objection to the age verification requirement, arguing that the obligation "would place multiple restrictions on minors' and adults' abilities to access covered websites and, in some cases, block access altogether." NetChoice has argued that the restriction is content-based, because the law applies to social media platforms and compels speech by requiring social media platforms to verify users' ages. NetChoice also has argued that the law's definition of targeted advertising is overly broad and not properly tailored to mitigate the potential impacts to free speech; in other words, NetChoice has argued that Louisiana has not shown that the age verification and advertising restrictions are necessary and narrowly tailored to address the impact of social media use on minors.

Source: *Lexology - Hunton Andrews Kurth LLP*

Wisconsin Supreme Court Tackles Thorny Contours of Arrest Record Discrimination

At a Glance

- Wisconsin Supreme Court took a broad view of what constitutes an arrest record for purposes of the state's employment discrimination law.
- Applicants and employees with non-criminal arrests can be protected under the anti-discrimination provisions, and exceptions to the law's protections are likely to be interpreted narrowly.

In a recent case, *Oconomowoc Area School District v. Cota*, the Wisconsin Supreme Court examined the definition of "arrest record" and the circumstances under which employers may lawfully consider arrest records in making employment decisions. As a practical matter, the decision is likely to increase the risk of employment claims by individuals subject to adverse employment actions in connection with arrest records in Wisconsin, though the case involved unique facts that may not apply in many situations.

Background of Existing Wisconsin Law on Arrest Record Discrimination
The Wisconsin Fair Employment Act (WFEA) generally prohibits employers from discriminating against applicants and employees on the basis of their arrest and conviction records.[1] It also generally prohibits employers from requesting information about an arrest record unless the arrest record is a pending charge.[2] Nevertheless, the law specifically allows employers to "refuse to employ . . . or to suspend from employment . . . any individual who is subject to a pending criminal charge if the circumstances of the charge substantially relate to the circumstances of the particular job."[3] In addition, preexisting case law in Wisconsin, *City of Onalaska v. LIRC*, 120 Wis. 2d 363, 354 N.W.2d 223 (Ct. App. 1984), had held that an employer that concludes from its own investigation that an employee has committed unlawful conduct and terminates the employee as a result of its own investigation does not engage in unlawful arrest record discrimination.[4]

Background Facts of the *Oconomowoc Area School District* Case
The employees at issue were members of the School District's grounds crew and, as part of their duties, recycled scrap metal for the School District. The employees, along with a coworker, brought scrap metal to a local processor, which paid with cash or checks made out to "cash." Their coworker reported that, approximately, two years prior, he and the employees delivered scrap metal to the processor but had kept the payment and split the money among themselves, *i.e.*, they stole from the School District.

The School District undertook an internal investigation into the alleged theft, but was unable to determine whether the

employees were responsible for the missing funds, and it did not take any adverse employment action against the employees at that time. Instead, the School District referred the allegations to local law enforcement. Ultimately, law enforcement did not uncover any new information implicating the employees. The employees were cited for municipal theft, which in Wisconsin is a non-criminal offense.

Approximately one year after the employees were cited for theft, an assistant city attorney informed the School District that he believed he could obtain convictions and that he also believed the case could be settled. The assistant city attorney proposed dismissing the citations against the employees in exchange for a $500 payment, which he characterized as "restitution." The School District indicated that it supported the proposal, but the employees had not agreed.

The next day, the School District terminated the employees' employment, claiming the School District had "learned" that the employees "were, in fact, guilty of theft of funds from the School District" and that they had lied about this during the School District's internal investigation. The municipal citations against the employees were ultimately dismissed. The employees never pleaded guilty to or were convicted of municipal theft.

After their termination, the employees filed administrative agency complaints alleging arrest record discrimination. The Wisconsin Labor and Industry Review Commission (LIRC) ultimately concluded that the School District had unlawfully discriminated based on their "arrest records." After the School District appealed, the circuit court affirmed the LIRC's decision, finding it was supported by "substantial evidence." The Court of Appeals reversed in the School District's favor, and the Wisconsin Supreme Court then took up review of the employees' appeal.

Wisconsin Supreme Court's Analysis

The first issue to be decided was whether the employees' municipal citation for theft was a qualifying "arrest record" under the WFEA's definition entitling them to protection under the law.

The School District argued that the employees did not have an "arrest record" because they were cited only for municipal theft, which is a non-criminal offense in Wisconsin. The definition of a qualifying arrest record "includes, but is not limited to, information indicating that an individual has been questioned, apprehended, taken into custody or detention, held for investigation, arrested, charged with, indicted or tried for any felony, misdemeanor or other offense pursuant to any law enforcement or military authority."[5] The Wisconsin Supreme Court rejected the School District's argument and held that the "any . . . other offense" language in the definition is broad enough to include alleged violations of both criminal and non-criminal laws. The conclusion was driven in part by the court's observation that Wisconsin law "expressly authorizes arrests in in connection with non-criminal offenses" such as for traffic violations. Thus, the Supreme Court held that the WFEA's "arrest record" discrimination protections apply to people arrested in connection with non-criminal matters, for example, municipal citations and non-criminal traffic offenses.

The second issue to be decided was whether the School District terminated the employees because of their "arrest record" under the unique circumstances of the case.[6] The School District argued that it terminated the employees' employment because of the conclusions from its own internal investigation, not because of their arrest records, and therefore the termination decisions were lawful. The School District's argument was based on *Onalaska*. The Wisconsin Supreme Court found the so-called *Onalaska* defense inapplicable, however, after determining that substantial evidence supported the conclusion that the School District was not motivated to act by its internal investigation. The court found compelling, among other things, that the School District had earlier concluded its internal investigation without being able to find that the employees had stolen, and that the only new events that had occurred thereafter—the municipal theft citations and the assistant city attorney's statements that he believed he could convict the employees and that he anticipated reaching a settlement—were part of the employees' "arrest records," not the School District's own internal investigation. Therefore, the Wisconsin Supreme Court affirmed the determination that the School District had violated the state's arrest record discrimination protections in terminating the employees.

What this Means for Employers

The *Oconomowoc Area School District* decision serves as a stark reminder that Wisconsin employers addressing situations involving applicant or employee arrest records should proceed cautiously. After the decision, it is clear that even applicants and employees with *non-criminal* arrests can be protected under the law and that exceptions to the law's protections are likely to be interpreted narrowly. When Wisconsin employers rely on their own independent

investigations of the underlying facts related to arrest records or pending criminal charges to make employment decisions, they must be cognizant of the substantial scrutiny LIRC and Wisconsin courts often place on such assertions. Employers should consider reviewing their practices related to the handling of such matters in Wisconsin to ensure that they can appropriately defend their employment decisions if challenged.

Source: *Lexology - Littler*

Getting Clear on Compiling Random Drug Testing Pools in Iowa

The Iowa Supreme Court recently clarified that a compliant random drug testing program under Iowa law requires excluding those who are not scheduled to work the day of the testing from the pool of employees who could be selected. *Hampe v. Charles Gabus Motors Inc. d/b/a Toyota of Des Moines et ano.*, No. 22-1599 (Iowa Sup. Ct. Apr. 11, 2025).

Iowa has one of the most technical drug testing laws in the country. It allows unannounced random testing of:

(1) The entire employee population at a particular work site of the employer except for employees not subject to testing pursuant to a collective bargaining agreement, or employees who are not scheduled to be at work at the time the testing is conducted because of the status of the employees or who have been excused from work pursuant to the employer's work policy prior to the time the testing is announced to employees.

(2) The entire full-time active employee population at a particular work site except for employees not subject to testing pursuant to a collective bargaining agreement, or employees who are not scheduled to be at work at the time the testing is to be conducted because of the status of the employee or who have been excused from work pursuant to the employer's working policy.

(3) All employees at a particular work site who are in a pool of employees in a safety-sensitive position and who are scheduled to be at work at the time testing is conducted, other than employees not subject to testing pursuant to a collective bargaining agreement, or employees who are not scheduled to be at work at the time the testing is to be conducted or who have been excused from work pursuant to the employer's work policy prior to the time the testing is announced to employees.

Iowa Code 730.5(8)(a).
In the case before the Supreme Court, the employer used a random testing pool that consisted of all employees. The employer did not exclude employees who were not scheduled to be at work at the time the testing was conducted or who were excused from work pursuant to the employer's policy. Instead, the employer had a list of alternate employees who could be tested if selected employees were not at work on the day the testing was conducted.

The Iowa Supreme Court held that this practice did not "substantially comply" with the law. Strict compliance with the law is not required, it explained, but substantial compliance is required. The Court held that the employer did not substantially comply with the law when it made no attempt to exclude employees who were not scheduled to be at work or because they had been excused pursuant to an employer policy.

Focusing on the plain language of the statute, the Court stated that it is the way the random pool is constructed that matters, even if, as a practical matter, it is difficult to comply with the statute's requirements given the "fluid circumstances" of today's workplace.

Source: *The National Law Review - Jackson Lewis P.C.*

INTERNATIONAL DEVELOPMENTS

PLEASE NOTE: Spellings of words in International articles such as those written in the British English format are native to the original author and differ from the spellings of words in the American English format.

Supreme Court Tightens Reporting Restrictions in Criminal Cases Involving Child Defendants (Ireland)

Last month, Ms Justice Iseult O'Malley, delivering judgment on behalf of a three-judge Supreme Court, overruled a landmark Court of Appeal judgment, which permitted the identification of a child defendant in the media once they turn 18, if criminal court proceedings or appeals are still ongoing. See the previous RDJ Insight here, which discusses the, now overruled, Court of Appeal decision on this matter.

Background
Ms Justice Isobel Kennedy found in the Court of Appeal that the defendant in the proceedings, who had been found guilty of the murder of Cameron Blair, could be named following reaching the age of majority. The defendant was 17 years old at the time of the incident on Bandon Road, Cork, on 16 January 2020. A long-standing interpretation of section 93 of the Children Act, 2001 ("**section 93**") was dislodged and reinterpreted following this Court of Appeal decision, such that the anonymity protection afforded to child offenders who are convicted, no longer protected these offenders as adults before appellate courts.

An order was made in the Court of Appeal to stay the naming of the defendant in the media, i.e., keep the reporting restrictions, in order to allow for a potential appeal to the Supreme Court. The defendant in this instance did bring this Supreme Court appeal.

The Appeal
It was specified by the Supreme Court that the crux of the appeal was whether a defendant who is brought before the courts as a minor, remains entitled to the protections of section 93 of the Act if they reach the age of 18 before the proceedings have concluded, to include any appeals. Lawyers for the defendant submitted that issues of fairness in exercising a right of appeal and concerns regarding the protection of children in the criminal justice system arise here.

Decision
The appeal was allowed, and it was ruled that anonymity protections should apply to a child at the commencement of criminal proceedings, throughout, and following conclusion of the proceedings. It was ruled that the prospect of losing the anonymity protection would inhibit a person's right to appeal.

Ms Justice O'Malley said that to interpret the section 93 anonymity protection as expired if the offender is still before the courts when they reach the age of 18, would be *"capable of creating an unjustifiable difference in the treatment of young persons engaged in the court process and has the potential to inhibit their rights of defence and appeal to an unnecessary and possibly damaging effect."*

Further, the Supreme Court judge held that by interpretating that the section 93 anonymity protection applied throughout and beyond the conclusion of proceedings seemed to her *"to reduce the possibility of unequal and unfair treatment as between young offenders and attempts to ensure that they are not subjected to additional, unjustified and unnecessary pressure and harm while involved in the criminal justice process."*

In arriving at this finding, the Judge noted that the Act placed particular emphasis on the rehabilitation of persons who commit crimes during childhood and that an objective of the legislation was to promote reintegration of child offenders into society.

The five-judge Supreme Court agreed unanimously with Ms Justice O'Malley's judgment and a declaration stating the anonymity protections shall apply to the defendant before all courts was granted.

Conclusion
Following this Supreme Court decision, child defendants in criminal proceedings will continue to enjoy the life-long anonymity protections afforded by section 93 of the Act, throughout and following proceedings, regardless of whether they

have "aged out" following a conviction, but before the conclusion of an appeal. The mainstream media, and indeed more casual users of social media, will need to be aware of this judicial shift in position that children charged with crimes and who age out during proceedings are no longer "fair game" to be named, unless the Court makes an order dispending with the anonymity protection afforded by section 93. It should be borne in mind that after the Ana Kriegel murder case a number of criminal prosecutions were brought against social media users who identified the boys convicted of her murder.

Source: *Lexology - RDJ LLP – Darryl Broderick and Aine O'Brien*

Europe - Pay Transparency Directive: preparing for the great unknown?

Over the last few months, we have done a lot of sessions with clients on the Pay Transparency Directive. Chief among the questions that inevitably comes up is implementation of the Directive in the different Member States. Clients wonder if and how they can prepare for June 2026 when – as per usual – most Member States are nowhere near presenting even draft legislation to translate the Directive into national legislation.

Our response to this entirely sensible question is always the same: while we will of course track local developments and keep you updated, please do not wait until there is more clarity from national legislators to take action on this topic. You don't have to know about every nut and bolt of the finished product to know enough to start your preparation, especially as the Directive does set out very clear pointers on the likely direction of travel.

One of the main principles of the Directive is that Member States should take the necessary measures to ensure that "*employers have pay structures ensuring equal pay for equal work or work of equal value*". These pay structures should be based on a job evaluation scheme which considers skills, effort, responsibility and working conditions (and, if appropriate, any other factors which are relevant to the specific job or position). There is no chance that those key indicators will be altered materially pre-implementation – while it is possible that some states may add further considerations, that will almost certainly be by way of illustration or expansion of those criteria, not variation of them. Making sure that the organisation has the right structures and schemes in place and determining the pay gaps in the organisation on this basis is a project that will likely take a couple of months, which does not leave an awful lot of time to remedy any gaps above 5% that would come out of the analysis.

And yes, the Directive does look to Member States to take the necessary measures to ensure that *"analytical tools or methodologies are made available to support and guide the assessment and comparison of the value of work in accordance with the [above] criteria"*. But in the current political climate, where even European Commission president Ursula von der Leyen has announced a drive for de-regulation, we do not expect that the Member States will be demonstrating excessive zeal when implementing this provision. Rather we expect that those which are already quite advanced on this topic – e.g. Spain, which has a public on-line job evaluation tool – will maintain what's already in place, whereas those less prepared Member States (which is the large majority) will likely leave it at the level of the principles set out by the Directive, without much more.

The first Member States that have issued draft legislation seem to confirm this prediction:

- **Sweden**'s existing legislation is already in line with the Directive's requirements, requiring employers to conduct annual reviews of equal jobs and jobs of equal value. Under the existing legislation, companies with 10 or more employees must document the salary review in writing, including specific measures to address any identified pay gap issues, while companies with 25 or more employees must also produce annual equality plans. The draft legislation to transpose the Directive is in fact a set of amendments to existing legislation:
- As per the Directive, employers must provide information to job applicants about the initial salary or range for the position. Sweden adds the obligation to offer information on any relevant collective bargaining agreement provisions on salary. Answering a question we also get quite often, the Swedish draft Bill specifies that this information does not need to be included in the job postings but should be provided in reasonable time to allow for an informed negotiation on pay. In line with the Directive, employers cannot ask prior salary history.
- Employers must inform employees about the "standards and practices" for wages, to help employees understand the annual equal pay salary reviews being conducted.
- Also in line with the Directive, employees must have rights to information on their individual pay level and average pay levels for workers performing equal work, broken down by gender.

- Employers with 100 or more employees must report gender pay gaps during the calendar year for the overall workforce to the Equality Ombudsman, who will publish this information. Employers must also report to the Ombudsman pay gaps by groupings of employees performing equal work, explaining differences of 5% or more with objective reasons or actions to be taken.
- Finally, the annual equal pay salary analysis must also include a comparison between women's and men's pay progression in connection with parental leave and pay progression for employees who perform equal work or work of equal value, compared to employees who have not taken a corresponding period of leave. This provision goes beyond Directive requirements, which only ask that family leaves be considered as part of a joint pay assessment (the further analysis imposed if the annual pay gap report shows a pay gap of 5% upwards in any given category).
- **Ireland**'s draft bill is less ambitious (though all credit to them for at least having started) as it only entails a partial implementation of the Directive. The draft Bill has a wider scope than the transposition of the Directive and includes two provisions relating to pay transparency:
- It requires employers to provide information about salary levels or ranges *in the job advertisement*. This requirement is slightly more restrictive than the Directive, which does not state that this information must be published (already) in the job advert. It is not clear in this stage exactly how detailed the information on pay range will need to be.
- In line with the Directive, the second measure prohibits employers from asking job applicants about their own pay history or their current rate of pay.
- In **Poland**, quite interestingly, Members of Parliament presented in December 2024 their own draft Bill, not waiting for the results from the governmental working group tasked with preparation for the implementing law. In February, the Polish Parliament (by a scarce majority of votes of 229 to 201 and against the majority of Ministries and institutions which commented upon on the draft Bill) decided to proceed with this draft while the other is in the early preparatory stages. The current draft focuses on implementing only parts of the Directive focused on:
- pay transparency: salaries and salary levels will not be confidential (no exceptions), and employees will have the right to request information on their individual salary levels and average salary levels; employer will not be able to prohibit or prevent an employee from disclosing information about their salary (not even if such disclosure may hurt business interest and is not necessarily focused on ensuring equal pay),
- pay transparency in recruitment: the employer, publishing information on an open job position, shall identify the proposed level of salary, indicating its minimum and maximum amount; similarly to Ireland, the employer is required to publish salary proposals in the "*information on possibility to hire an employee on a specific job position*" (which we understand to mean the job advertisement), and there is no flexibility as to how and when this information is to be provided to the candidate.
- pay progression information: employer shall provide the employee with access to the criteria used to determine employee salary and pay progression; such criteria must be objective and gender-neutral; the draft Bill suggests that employers with fewer than 50 employees "*may be released from this obligation".* It is not, however, clear by whom.
- new penalties will be imposed on employers in Poland for not informing employees of their salary level when requested, for not publishing information on salary in job advertisements and for employing an employee at a salary lower than stipulated in the job posting. This raises a number of questions, e.g. what if the salary is lower because the parties agreed to proceed with a part-time employment or to a reduction in scope of responsibilities? Will this still be a punishable offence?

The draft Bill is rather short and it does not touch upon sensitive topics such as job evaluation, objective or gender-neutral criteria for differentiation of salaries, or gender pay gap reporting. These matters are expected to be comprehensively regulated only in the governmental Bill, which is still a "work in progress" and not expected any time soon. It is fair to say that no guidance may be taken from the draft Bill as proposed, and at places it is actually quite confusing.

- Finally, in **Germany**, the interim Minister for Family, Senior Citizens, Women and Youth, Lisa Paus, has apparently announced in a private meeting a couple of months ago that Germany will likely go for continued flexibility in setting categories of workers without imposed pay evaluation systems. Germany will also focus heavily on the Right to Information, which already exists but will be strengthened in the framework of the transposition process. This information is however not yet confirmed on the interim Minister's website. At the moment, it is unclear whether this approach will be continued because the Green Party, of the which the interim Minister is a member, will no longer form part of the new government. It is uncertain what the priorities of the new government will be when implementing the Directive. We will keep you updated.

In summary, only four Member States have allowed us a view into their thinking on Pay Transparency Directive implementation, but in none of the four cases is the output of such a nature that it should prevent companies from making a start on the biggest chunk of the work, around fair job evaluation and the assessment and analysis of the gaps as they present themselves on the basis of such job evaluation. The time is now, more than ever.

Source: *Lexology - Squire Patton Boggs- Marga Caproni, Laura Sparschuh and Malgorzata Grzelak*

South Africa Introduces Mandatory e-Portal Reporting for Data Breaches

On April 7, 2025, South Africa's Information Regulator announced a new requirement for organizations to report data breaches—referred to under local law as "security compromises"—via an online eServices Portal. The announcement marks a significant procedural shift in how companies must comply with the Protection of Personal Information Act, 2013 ("POPIA"), South Africa's data protection framework.

The move to a digital platform aligns South Africa with international trends toward streamlined breach reporting mechanisms. For companies that process personal information using means located in South Africa—whether or not they are headquartered in the country—this development highlights the importance of understanding when and how POPIA may apply. Foreign-based companies that rely on South African infrastructure, service providers, or operations to process data should review whether their activities fall within POPIA's extraterritorial scope.

POPIA and the Concept of a "Security Compromise"
POPIA defines a "security compromise" broadly as any unauthorised access to, or acquisition of, personal information. While this may sound similar to the concept of a "data breach" in the EU General Data Protection Regulation ("EU GDPR"), the terminology and legal framework in South Africa differ in several key respects.

Under POPIA:

- A "responsible party" (analogous to a data controller in EU or UK data protection law) is the person or entity that determines the purpose and means of processing personal information
- An "operator" (akin to a data processor) is a third party that processes information on behalf of the responsible party under contract
- Both responsible parties and operators must take "appropriate, reasonable technical and organisational measures" to safeguard personal information and prevent unauthorised access, damage, loss or destruction

If a responsible party has reasonable grounds to believe a security compromise has occurred, they are required to notify both the Information Regulator and the affected data subjects as soon as reasonably possible.
The notification to data subjects must include:

- A description of the possible consequences of the breach
- A description of the measures taken or to be taken by the responsible party to address the breach
- Recommendations on how data subjects can mitigate potential adverse effects
- If known, the identity of the unauthorised person who may have accessed or acquired the personal information

There are limited exceptions that allow a delay in notification—for example, where immediate notice would impede a criminal investigation by law enforcement.

New Reporting Mechanism: eServices Portal
The Information Regulator's new online eServices Portal serves as the official platform for submitting breach notifications. It is still unclear whether reporting via the official platform fully replaces the use of Form SCN1, the Information Regulator's prescribed form for manually reporting security compromises, first released in 2023, but Information Officers are encouraged to submit their reports digitally via the portal going forward.

According to the Information Regulator's announcement, the portal aims to:

- Simplify the submission process for Information Officers, a statutory role under POPIA assigned to a senior individual within an organization and functionally comparable to a Data Protection Officer under the EU GDPR and similar global frameworks
- Improve the Regulator's ability to monitor and respond to breach notifications

- Standardize the quality of information submitted in response to security incidents

Does POPIA Apply to Foreign-Based Organizations?
Although POPIA does not explicitly provide that it has extraterritorial application, its reach extends beyond South African borders in certain instances. A company that is not domiciled in South Africa may still be subject to POPIA if it makes use of automated or non-automated means in the country to process personal information, unless those means are used solely for transit through the country.

The potential extraterritorial scope means that foreign-headquartered companies may fall within POPIA's regulatory ambit in scenarios such as:

- Using South African-based vendors or IT infrastructure to store or process data
- Outsourcing HR, payroll, or customer support functions to South African service providers

In these situations, such companies may be required to *inter alia*:

- Comply with POPIA's principles, including security safeguards and breach notification requirements
- Designate an Information Officer to *inter alia* serve as a point of contact for the Information Regulator and affected data subjects

While POPIA shares similarities with frameworks such as the GDPR, including in its extraterritorial reach and underlying privacy principles, it also contains South Africa-specific obligations and enforcement mechanisms. Multinational organizations should therefore assess their exposure under POPIA independently and avoid relying solely on global privacy programs.

Implications and Next Steps
The rollout of the eServices Portal signals the Information Regulator's continued efforts to operationalise POPIA and strengthen its enforcement infrastructure. It also underscores the expectation that organizations subject to POPIA take a proactive and structured approach to managing data breach responses.

For international organizations—particularly those without a physical presence in South Africa—this development is an opportunity to revisit how personal information from or about South African individuals is processed, stored, and secured. It may also be a trigger to assess whether POPIA compliance obligations apply, and whether existing incident response plans account for the nuances of local law.

Source: *Lexology - Covington & Burling LLP – Dan Cooper, Benjamin S Haley, Deon Govender, Ahmed Mokdad and Mosa Mkhize*

Pay Equity Blitz Audits Are Coming for Federally Regulated Employers (Canada)

Over the past few years, federal employers with 10 or more employees have been engaged in the important but time-consuming process of developing their initial pay equity plan as required by the new *Pay Equity Act* (the "Act").[1] Many employers – particularly non-unionized employers – were able to finalize and post their initial pay equity plans by the September 3, 2024 deadline. Others have applied for and been granted extensions by the Office of the Pay Equity Commissioner (the "Commission") (see our bulletin for more information on the extension process).

With the initial deadlines behind them for most employers, the Commission recently advised that it will launch a "blitz audit," to verify compliance with the *Act*.

In this update, we review the information provided by the Commission concerning its intention to conduct blitz audits and what employers can do to prepare.

An Introduction to Pay Equity Audits
A pay equity audit, distilled to its most basic, starts and ends with one simple question: what have you done to comply with your pay equity obligations? According to the *Act*, the Commission can conduct two different types of audits to confirm compliance with the *Act*: internal audits and compliance audits. Both types of audits are described below.

1. Internal Audits: The Commission can order that an employer conduct an "internal audit" and provide the Commissioner with a report of the audit results.[2] Where an internal audit is ordered, it may take one of two forms. A "standard" audit is an internal audit that focuses on one employer or bargaining agent and on at least one line of enquiry. On the other hand, a "horizontal" audit is an audit that focuses on one industry or sub-industry and specific lines of enquiry. Horizontal audits examine issues across many employers in a selected industry. The *Act* is silent on the type of auditor (i.e. internal or external) that an employer can use to conduct an internal audit. However, the Commission advised that employers can choose who will undertake the audit, and that a third-party consultant can be selected.[3] The Commission has also confirmed that internal audits will be subject to monitoring mechanisms to ensure the integrity of the audit, including, for example, that the audit must be shared with the Commission for review.[4] If, while conducting an audit, an employer learns that it has violated the *Act* or Regulations referenced in the Commission's order, it must indicate these violations and that measures that have been taken to correct them in its report to the Commissioner.[5]
2. Compliance Audits: This is an audit that is led by the Commissioner regarding any employer or bargaining agent.[6] The purpose of a compliance audit is in the name: to ensure compliance with all provisions of the *Act* or its Regulations.

Blitz Audits: What Are They?

A blitz audit is a type of "compliance" audit that is led by the Commission and is focused only on one or two requirements of the *Act* and the Regulations. According to the Commission, a blitz audit has the following objectives:

- ensure compliance with the *Act* and Regulations;
- ensure that employers are aware of their obligations under the *Act* and inform employers of what is required to comply, if not in compliance; and
- promote the Commission's tools and publications.[7]

The blitz audit process is expected to include the following five general steps:[8]

1. Notification Letter: The Commission will notify employers who have been selected for an audit as part of the blitz audit. The notification letter will include details and timelines about the audit and the information to be provided to the Commission for review.
2. Submission of Documents: The employer will submit all requested information to the Commission for review, according to the timelines provided. The Commission has stated that it is still finalizing operational details concerning the audit process, including whether employers will be allowed to make requests for extensions during the audit process. However, it has confirmed that it intends to take a "case-by-case" approach to addressing extension requests.
3. Review and Assessment: The Commission will review all information submitted by selected employers and make an assessment regarding compliance with the *Act*.
4. Letter: The Commission will mail a letter to the employer with the Commission's findings concerning the blitz audit.
5. Corrective Measures: If a blitz audit reveals non-compliance with the *Act*, corrective measures may be taken by the Commission. The Commission has stated that administrative monetary penalties are one tool that can be used to encourage compliance, in addition to other tools such as voluntary compliance and compliance orders.

The Commission has confirmed that the first blitz audits it will conduct will focus on the following two requirements of the *Act* and Regulations:

1. Did the employer establish and post a pay equity plan in accordance with the *Act*?
2. Were increases in compensation implemented as per the results of the pay equity plan and in compliance with the *Act* and its Regulations?[9]

The Commission has confirmed that the audit criteria includes the posting of the pay equity plan and date of posting and the posting schedule of increases in compensation and date of posting. We note that the Commission's verification of the first requirement – i.e. the establishment of a pay equity plan in accordance with the *Act* - could be interpreted very broadly or more narrowly, depending on the approach taken by the Commission. For example, the Commission could simply request a copy of the plan or, it could require further information concerning all elements contained within a plan to verify whether the methodology applied conforms with the *Act*.

Preparing for the First Blitz Audit

The Commission advised that the first blitz audit would begin by the end of March 2025, however, the Commission has not yet confirmed an exact date for the launch. The Commission also stated that it expects to complete the first blitz audit prior to the deadline for the first annual statement, which is due on June 30, 2025[10] (see our bulletin for more information on the annual statement process).

The Commission has explained that the first blitz audit will target employers that have *not* received approval for an extension to post a final pay equity plan. The Commission has explicitly stated that it does *not* intend to audit employers that were granted an extension to post their pay equity plans during the blitz audit since it expects them to focus on the work they need to perform to establish their pay equity plan.[11]

In order to prepare for the first blitz audits, employers should consider:

- Collecting copies of the required postings (e.g. initial notice, draft pay equity plan notice, notice of final plan and notice of increases to compensation), the initial pay equity plan itself and details of where the various postings were made, to ensure they are ready to share with the Commission if requested; and
- Compiling notes from the employer's pay equity committee and other documentation that supports the work of the initial pay equity plan, should they be required.

If any potential concerns arise during the course of a blitz audit, employers should immediately contact legal counsel to discuss and strategize potential solutions, under privilege.

Source: *Lexology – Fasken - Jackie VanDerMeulen, Sophie Arsenault, Carl Trudeau and Rebecca Rossi*

MISCELLANEOUS DEVELOPMENTS

GDPR and Geolocation of Professional Vehicles (Belgium)

In a recent decision, the Belgian Data Protection Authority (DPA) reviewed an employer's use of geolocation system company vehicles. An employee challenged the practice, arguing that he had neither given consent nor had the ability to deactivate the device outside working hours, during holidays and sick leave.

The DPA examined key aspects of this issue, particularly the legitimacy of data collection and compliance with the principles of transparency and purpose limitation.

Key principles

- **Legitimate interest, but clear purpose:** The DPA confirmed that employers may justify the use of geolocation systems based on legitimate interest, such as tracking working hours, optimizing travel, and reducing costs. However, the employer should have explicitly defined the system's purpose – in this case, tracking working hours.
- **Data Minimization and Proportionality:** The DPA found that the continuous recording of location data, including outside working hours, was disproportionate. Employers should implement solutions that allow employees to deactivate tracking outside working hours.
- **Enhanced transparency obligations:** The DPA criticized the employer's geolocation policy for being vague and ambiguous. To ensure compliance, employers must provide clear and precise information on how geolocation data is collected, stored, and used, eliminating any room for interpretation.
- **Balancing employer needs with employee rights:** While the DPA acknowledged that restricting access to geolocation data during working hours limited the impact on employees' privacy, it emphasized the need for a system that better respects individual freedoms.

Recommendations for Employers

To ensure compliance with GDPR and best practices in geolocation tracking, employers should:

- **Clarify the purpose of geolocation:** Clearly define the systems' objectives (e.g., tracking working hours) and ensure they align with a legitimate interest.
- **Enhance transparency:** Provide employees with detailed documentation on date collection, processing and usage.
- **Limit data collection:** Enable employees to deactivate geolocation tracking outside working hours or implement a technical mechanism to restrict continuous tracking.
- **Conduct a data protection impact assessment:** Assess potential risks for employees before deploying a geolocation system and implement necessary safeguards.
- **Ensure compliance with internal policies:** Regularly review and update the geolocation policy to align with evolving data protection requirements.

Source: *Lexology – Strelia – Stefanie Tack and Aylin Ozturk*

Is Marijuana as Dangerous as Alcohol for Drivers (Canada)?

The effects and serious consequences of driving while impaired by alcohol are widely known. What may not be as appreciated is the similar effect that marijuana can have on drivers. Due to this, driving while high does not carry the same stigma as driving while drunk does. As the recreational use of marijuana products becomes more popular, it is important to highlight the underappreciated road safety concerns that are raised by driving while high.

Driving under the influence of marijuana, even for someone who is normally a skilled and cautious driver, can significantly impair their ability to operate their vehicle safely in several ways. Firstly, it can impair the driver's reaction time. A high driver may experience an altered perception of time and feel as though they have a longer chance to react to road hazards such as breaking cars, changing lights, crossing pedestrians, etc. Their spatial perception may also be affected which can lead to a driver making risky decisions such as merging with traffic when it is not safe to do so or following too close.

Another symptom of marijuana is difficulties in focus and concentration. A high driver may have trouble staying focused

on the road while processing multiple stimuli. This leaves them at a heightened vulnerability for distraction by things such as incoming text messages, chatting passengers or sights passing by their window, all of which divert their attention away from the road.

Fatigue is another side effect of marijuana use. Even slight drowsiness can dramatically impair a driver's ability to keep their vehicle under control or stay alert to respond to hazards quickly.

Aside from the dangers of driving while high, the legal consequences are significant. Police can use roadside testing such as standard field sobriety tests and oral fluid screening devices that allow them to easily test for cannabis in drivers. Much like for alcohol, there is a zero-tolerance standard for having consumed marijuana for commercial drivers, drivers under the age of 21, and those who have a G1 or G2 class licence. Any cannabis found in these drivers' systems can result in license suspensions and high monetary fines. As for non-commercial drivers holding class G licenses the prohibited level of cannabis is 2 nanograms of THC pel milligram of blood. Visit Cannabis and driving | ontario.ca for more information about legal prohibitions on driving while high.

It is not a constructive exercise to compare the effects of alcohol and marijuana on drivers from a perspective of which one is more/less dangerous. Both substances can impair your ability to drive creating dangers for you and those you share the road with. When engaging with alcohol or cannabis, the safest course is always to arrange a sober (and safe) drive home.

Source: *Lexology - Oatley Vigmond LLP- Bennett Dawson*

Mexico Overhauls Federal Data Protection Law

Isabel Davara F. de Marcos of Davara Abogados S.C. reports that on March 20, 2025, the Mexican Congress approved a new Federal Law on the Protection of Personal Data Held by Private Parties ("LFPDPPP"), replacing the previous 2010 federal data protection law. The LFPDPPP, which became effective March 21, 2025, represents a substantial change in Mexico's data protection framework, impacting the scope of application, legal bases for data processing, and individual rights. Relevant updates and considerations for companies operating in Mexico include:

- expanded definition of personal data;
- broader legal bases for processing;
- stricter privacy notice requirements;
- enhanced individual rights over automated processing; and
- increased fines and a new judicial structure (i.e., the creation of specialized data protection courts to handle legal proceedings, including constitutional rights lawsuits).

The LFPDPPP dissolves the National Institute for Transparency, Access to Information and Personal Data Protection, transferring its authority to a newly created Secretariat of Anti-Corruption and Good Governance. This body will oversee compliance, conduct investigations, and impose sanctions.

Promulgating regulations are expected to be issued within 90 days from the law's effective date, which are expected to clarify the scope and operational details of the law.

Source: *The National Law Review - Hunton Andrews Kurth LLP*