NOVEMBER 2024

CLEARSTAR®

SCREENING COMPLIANCE UPDATE

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

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

CLICK FOR PAST UPDATES

TABLE OF CONTENTS

SCREENING COMPLIANCE UPDATE | NOVEMBER 2024

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

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

November 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: The Department of Labor (DOL) announced the publication of the "AI & Inclusive Hiring Framework" to "support the inclusive use of artificial intelligence in employers' hiring technology and increase benefits to disabled job seekers."
- STATE DEVELOPMENTS: The New York Clean Slate Act took effect to provide for the automatic sealing of certain criminal convictions after a specified time period and require greater disclosure by employers of criminal history information being considered in connection with hiring or continued employment.
- INTERNATIONAL DEVELOPMENTS: Ontario (Canada) plans to ban registered sex offenders from changing their names as individuals who are on the provincial sex offender registry will no longer be allowed to legally change their name once new legislation is passed.

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.

PLEASE NOTE: ClearStar does not provide or offer legal services or legal advice of any kind or nature. Any information contained in this Screening Compliance Update or available on the ClearStar website is for educational purposes only.

FEDERAL DEVELOPMENTS

DOL's AI Hiring Framework Offers Employers Helpful Guidance on Combatting Algorithmic Bias

On 24 September 2024, the Department of Labor (DOL) announced the publication of the "AI & Inclusive Hiring Framework" (Framework) to "support the inclusive use of artificial intelligence in employers' hiring technology and increase benefits to disabled job seekers."[1] The Framework is one of the latest publications designed to support the Biden-Harris administration's "Blueprint for an AI Bill of Rights", which focuses on how artificial intelligence (AI) may exacerbate existing biases in employment, housing, education, and other key legal areas.[2] The DOL also issued comprehensive guidance on best practices on using AI tools in the workplace on 16 October 2024, which we will address in a forthcoming alert.

The Framework was published by the Partnership on Employment & Accessible Technology (PEAT), a private entity funded by the DOL's Office of Disability Employment Policy (ODEP), and was primarily authored by ODEP and PEAT, with the National Institute of Standards and Technology's and other external partners' assistance.[3] Although the DOL and ODEP were involved in the Framework's drafting and promotion, PEAT's website makes clear that the Framework "does not necessarily reflect the views or policies of ODEP or DOL."[4] Despite this disclaimer, the Framework provides helpful guidance for employers seeking to responsibly, equitably, and legally use AI in hiring.

Framework Focus Areas
The Framework contains 10 focus areas and associated goals, with guidance and resources provided by PEAT as to each focus area and goal.

Identify Legal Requirements
Including determining the applicable state and federal laws regarding nondiscrimination, accessibility, and privacy that would affect AI hiring technology

Establish Staff Roles
Including selecting and training workers who will deploy AI hiring technology

Inventory Technology
Including collecting information from vendors about the use of AI hiring technology

Work with Vendors
Including creating and implementing policies with the vendors to ensure inclusive deployment of the AI hiring technology

Assess Impacts
Including evaluating the positive and negative effects of the AI hiring technology alongside internal and external stakeholders

Provide Accommodations
Including developing a process for job seekers to request accommodations

Use Explainable AI
Including writing plain language statements for job seekers about the AI hiring technology and how they can request accommodations

Ensure Human Oversight
Including drafting guidelines for using the AI hiring technology and measure the human performance in using the AI hiring technology tools

Manage Incidents
Including creating policies and systems for recording, responding to, reporting, and appealing identified incidents

Monitor Regularly
Including reviewing the performance of the AI hiring technology tools

To avoid overwhelming employers, employees, and job seekers, the Framework makes clear that the goals are meant to be implemented in stages and are not designed to be tackled immediately all at once.

The Framework also shares some policy goals with other federal guidance on AI in the labor and employment space. For example:

- Focus area 5 assesses the impact AI may have on current and prospective employees among others and mirrors the overarching goal of the US Equal Employment Opportunity Commission's (EEOC) 18 May 2023 nonbinding guidance on AI-influenced "selection procedures" (e.g., hiring, firing, promoting, etc.) and how it may trigger Title VII disparate impact liability;[5]
- Focus area 10 notes the importance of regularly monitoring AI tools to ensure compliance with nondiscrimination and accessibility legal requirements, which the Office of Federal Contract Compliance Programs (OFCCP) also highlighted in its 29 April 2024 nonbinding guidance on AI use by federal contractors.[6]
- Focus areas 4, 6, 7, and 8 also contain considerations addressed in the OFCCP's guidance, including that: (i) legal liability relating to the use of AI tools ultimately rests with the employer and cannot be assigned to the AI vendor; (ii) employers should have a process for applicants to request accommodations relating to the use of AI; and (iii) employers should create human oversight policies and procedures.[7]

Recommendations
Employers considering using or already using AI when making key employment decisions (e.g., hiring, firing, promotions) should consult the Framework and ensure that their AI programs address the 10 focus areas. Further, if employers also have frequent contact with other federal agencies, such as the OFCCP because of federal contracts they possess, then they should also consult that agency's respective AI guidance. Additionally, while federal agencies have acted in Congress's absence on AI, states have also proposed — and in some cases enacted — legislation regulating AI. Employers and their counsel should track state AI-related developments and ensure compliance to avoid legal and reputational risks.

CLICK HERE FOR SOURCE ARTICLE

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

NJ State Assembly Passes Pay Transparency Legislation

Synopsis: *New Jersey is positioned to join the growing number of jurisdictions that have adopted pay transparency requirements. The New Jersey State Assembly recently passed Senate Bill 2310, which, if enacted, will require employers to include a pay range in job postings and provide notice of promotional opportunities to current employees. The bill awaits the Governor's signature.*

On September 26, 2024, the New Jersey Legislature passed Senate Bill 2310. If signed into law, the bill will require employers to:

1. Make reasonable efforts to announce, post, or otherwise make known advertised opportunities for promotion to all current employees in the affected department(s) of the employer's business prior to making a promotion decision; and
2. Disclose in each posting for new jobs and transfer opportunities the hourly wage or salary, or a range of the hourly wage or salary, and a general description of benefits and other compensation programs for which the selected candidate would be eligible in the first 12 months of employment.

S2310 is currently awaiting New Jersey Governor Phil Murphy's signature. The law would become effective seven months after its enactment.

Which Employers Are Covered Under the Law?
The bill broadly defines a covered "employer" as any person, company, corporation, firm, labor organization, or association which has 10 or more employees in over 20 calendar weeks and does business, employs persons, or takes applications for employment within the State of New Jersey. Job placement, referral agencies, and other employment agencies are included in the definition of "employer" under the current draft of the bill.

What Must Employers Disclose and What Job Postings Are Covered?
The bill addresses two distinct requirements. First, a "notice" requirement to internal employees in an impacted department for promotion decisions. Second, the disclosures that must be included in a job posting for a new job, promotion or transfer opportunity. Both requirements cover both internal and external advertisements.

First, where an employer advertises opportunities for a promotion either internally or externally, the employer must make "reasonable efforts" to announce, post, or otherwise make known such promotional opportunities to all current employees in the affected department or departments of the employer's business prior to making a promotion decision. The law defines promotion to mean "a change in job title and an increase in compensation." As written, the bill's notification requirements are triggered when an employer advertises a promotional opportunity internally within the employer or externally on internet-based advertisements, postings, printed flyers, or other similar advertisements. The notification requirements would not apply if a current employee is awarded a promotion based on years of experience or performance. The language of the bill is vague as drafted, but likely intends to exclude non-competitive "in-line" or progression promotions. The bill also includes an exception for promotions on an "emergent basis due to an unforeseen event" – under those circumstances, no notice to current employees is required before making the promotion decision.

Second, the law covers the information that must be included in job postings for new jobs and transfer opportunities. In such postings, the employer must disclose the hourly wage or salary, or a range of the hourly wage or salary. The employer must also include a general description of benefits and other compensation programs for which the selected candidate would be eligible. The bill specifies that an employer may offer an applicant higher wages, benefits, and other compensation than that indicated in the posting. Interestingly, "transfer opportunities" is not defined. Presumably, a transfer would only apply to internal employee job moves, and could include promotions. However, the term "promotions" was expressly excluded from the final version of Section 1(b) of the bill. Additional clarification regarding this provision from the Department of Labor and Workforce Development would be welcomed if the bill is signed into law, as employers will have practical challenges in implementing such a requirement.

Temporary Help Service and Consulting Firm Exception
The law includes an exception for temporary help service firms and consulting firms registered with the Division of

Consumer Affairs in the Department of Law and Public Safety. For job postings that are posted for the purpose of identifying qualified applicants for potential future job openings – and not existing job openings – such firms are not required to include the standard pay and benefits disclosures. Such firms, however, must provide the pay and benefit information to an applicant for temporary employment when they are interviewed or hired for a specific job opening.

Enforcement and Potential Penalties
The proposed law would be enforced by the Commissioner of Labor and Workforce Development in a summary proceeding. Employers found to have violated the law will be subject to civil penalties in the amount of $300 for a first violation, and $600 for each subsequent violation. The bill does not contemplate a private right of action.

Under the proposed law, an employer's failure to comply with the promotional opportunity notification requirements will be considered one violation for all listings of a particular promotion, even if that promotion is listed on multiple forums. With respect to the pay and benefits disclosure requirements, an employer's failure to comply for all postings for a particular job opening or transfer opportunity will be considered one violation regardless of the number of postings that list, or forums that advertise, that job opening or transfer opportunity.

CLICK HERE FOR SOURCE ARTICLE

New York Clean Slate Act Takes Effect on November 16, 2024, With New Obligations for Employers Running Criminal Background Checks

On November 16, 2024, the New York Clean Slate Act (the "Act") will take effect. The Act provides for the automatic sealing of certain criminal convictions after a specified time period. It will also require greater disclosure by employers of criminal history information being considered in connection with hiring or continued employment.

Specifically, the Act provides that the New York State Unified Court System has up to three years from the effective date (that is, until November 16, 2027) to seal all eligible convictions. At that point, going forward, all eligible convictions will be automatically sealed and will become unavailable to most employers that conduct background checks as part of the hiring process or otherwise in the course of employment.

Convictions Eligible for Sealing
Convictions for most misdemeanor and felony convictions are eligible to be sealed. However, certain convictions, such as sex offenses, sexually violent offenses, and non-drug-related Class A felonies, including murder, are not eligible for sealing under the Act.

Time Period Before Convictions are Sealed
Misdemeanor convictions are eligible to be sealed three years from the date of sentencing (if no sentence of incarceration was imposed), or three years from the date of the individual's release from incarceration, whichever is later. Felony convictions are eligible to be sealed eight years from the date of sentencing (if no sentence of incarceration was imposed), or eight years from the date of the individual's release from incarceration, whichever is later.

For a conviction to be sealed, the individual must not currently be on parole, probation, or post-release supervision. Moreover, if the individual incurs a new misdemeanor or felony conviction before their prior conviction is sealed, the waiting period starts over and reflects the most recent conviction. The prior conviction is only sealed once the waiting period for the most recent conviction is complete.

Exempt Employers
Employers that are otherwise required by law to conduct "fingerprint-based" criminal history checks, such as employers in childcare, eldercare, and disability care, will have access to records that would otherwise be sealed under the Act.

Employer Notice Requirements
The Act also imposes heightened notice obligations on employers conducting background checks that include criminal history information. Employers that receive criminal history information as part of a background check will now be required to furnish a copy of the report containing such information to the applicant and notify the applicant of their right to "seek

correction of any incorrect information contained [therein]." This information must be provided along with a copy of Article 23-A of the New York Correction Law, which employers are already required to furnish to applicants as part of the criminal history background check process under law.

Importantly, employers must abide by the above notice requirement regardless of whether the employer plans to take adverse action against the applicant based on their criminal history. This is a change from the current process whereby criminal history information obtained as part of a background check need only be disclosed by an employer if adverse action is intended to be taken.

Protections Against Negligence Claims for Employers

Because many criminal convictions will be sealed, the Act provides non-exempt employers with a defense against negligent hiring, retention, and supervision claims. If, for example, an employer conducts a background check on an applicant and the criminal history report did not contain any convictions because the convictions were sealed, and the employer hired the applicant who then engaged in some type of wrongful behavior at work, the Act would prohibit potential litigants from introducing the sealed convictions as evidence of negligence against the employer because the employer had no knowledge of such convictions.

However, employers exempted under the Act (as described above) that receive records that would otherwise be sealed as part of a background check owe a duty of care to individuals with sealed convictions and can be liable for negligence under Section 50-G of the New York Civil Rights Law if they (i) "knowingly and willfully" breach that duty of care by disclosing the sealed records without the individual's consent, (ii) the disclosure causes injury to the individual, and (iii) the employer's breach of their duty of care was a "substantial factor in the events that caused the injury suffered" by the individual.

CLICK HERE FOR SOURCE ARTICLE

Maryland DOL Adds to Its Guidance on the New Pay Transparency and Paystub Notice Obligations

As of October 1, 2024, employers with Maryland employees are subject to new wage range posting and paystub notice obligations, as detailed in our April 10, 2024 E-lert. In September, the Maryland Department of Labor issued FAQs and other resources to assist employers in complying with the new obligations, which we discussed in our September 11, 2024 E-lert. And now the MDOL has added to those FAQs.

Background on Wage Transparency Requirement. Maryland's Equal Pay for Equal Work Act now imposes more expansive disclosure obligations on employers, 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.

The Wage Transparency Guidance: The MDOL has updated its FAQs to make the following points:

- The law applies only to postings made on or after October 1, 2024, but employers must comply with the law for any reposted positions after October 1.
- All solicitations, whether internal or external, are covered, including but not limited to the following: newspaper ads and printed flyers; social media posts; and e-mails sent to multiple applicants or through an electronic mailing list.

- The law does not require employers to post all job opportunities; it only requires employers to comply with the law if they post an opening.
- Employers may use a "Help Wanted" sign on a vehicle or building as long as applicants are subsequently provided with or can readily access the required information. A sign could have a website address or QR code that links to the required information. Employers can email the information to online applicants or hand a document with the information to walk-in applicants.
- If the employer is offering a single fixed rate, the posting would include the fixed rate.
- Employers may have a link in a posting to the wage range and benefits, as long as all required information is included in the link and it is easily accessible.

Background on the Paystub Notice Requirement. The physical paystub or the online pay statement must now contain extensive and specific required information, to 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.

The Paystub Notice Guidance: The MDOL has added the following information of significance to its FAQs on the paystub or pay statement notice:

- The law applies to workers subject to a collective bargaining agreement.
- The notice does not need to list the hours worked for employees who are overtime-exempt under federal and state law.
- The paystub law does not require leave balances to be included on the notice, but the Maryland sick and safe leave (SSL) law separately requires employers to provide a written statement of each employee's SSL balance with each paycheck. According to the MDOL, the best practice would be to include the SSL balance on the notice.
- No notice is required if the employee worked no hours during the pay period and will not receive any wages (as paid time off or otherwise).
- A notice generated by a third-party processing company must still include the name of the actual employer.
- In cases involving joint employers or parent-subsidiary companies, employers should consult with legal counsel about which employer(s)'s name should be listed on the notice.

CLICK HERE FOR SOURCE ARTICLE

New York Passes the Equal Rights Amendment for Public Employers

New York voters just passed Proposition One, also called the New York Equal Rights Amendment, expanding protections under the state constitution's equal protection clause for public employers. The state constitution will now prohibit discrimination based on race, color, ethnicity, national origin, age, disability, creed, religion or sex—including sexual orientation, gender identity, gender expression, pregnancy, pregnancy outcomes and reproductive healthcare and autonomy.

What does this mean for NY employers?

The Amendment *will not* impact private employers as the state constitution's equal protection clause does not apply to private employers. However, other New York State and NYC laws have and continue to prohibit employment discrimination based on the above protected categories.

CLICK HERE FOR SOURCE ARTICLE

What Illinois Employers Using E-Verify Should Know About the New Requirements Effective 2025

An amendment to the Illinois Right to Privacy in the Workplace Act going into effect on Jan. 1, 2025, imposes many new obligations on employers regarding the use of E-Verify – some that go beyond federal E-Verify requirements. The Illinois Department of Labor (IDOL) has published guidance on the law that also clarifies that the law does not ban the use of E-Verify in Illinois. The new law includes strict deadlines for employer notifications and attestations, among other

requirements.

In addition to clarifying that E-Verify can be used in Illinois, the new guidance:

- Urges employers using E-Verify to familiarize themselves with information on the IDOL website about the accuracy of E-Verify;
- Prohibits misuse of E-Verify, including for pre-screening;
- Encourages employers to review and understand their legal responsibilities regarding posting and notice requirements;
- Reminds employers that employees may file complaints for alleged violations with IDOL; and
- Explains that any adverse action against an employee or applicant who files a complaint under the Right to Privacy Act is prohibited.

Illinois employers will violate state law by:

- Failing to display E-Verify notices supplied by the federal and Illinois state governments;
- Failing to have all employees who use the system participate in the required computer-based training;
- Failing to prevent employees from circumventing the training requirement;
- Misusing E-Verify in any way including using the system for pre-screening or screening current employees;
- Failing to safeguard the information in the system and preventing unauthorized access; and
- Failing to follow the notification and attestation requirements in the law.

The law imposes on employers notification and attestation requirements that are particularly detailed.

Here are just some examples:

- Upon initial enrollment in E-Verify or within 30 days of the effective date of the amendment (Jan. 1, 2025), the employer must file an attestation that they have received all the training materials and that they will do the training, post the required notices, and retain all certifications of completion of training for possible inspection.
- If the employer contends there is a discrepancy in the employment verification documents provided by an employee, the employer must explain the specific deficiency to the employee, provide the employee with instructions as to how to correct the deficiency, explain that the employee has a right to representation, and, upon request, provide the original document that provides the basis for the deficiency within 7 business days.
- When an employer receives a notification of a discrepancy from a state or federal agency:
    - Employer cannot take any adverse action including re-verification based on the notification.
    - Employer must provide notification to the employee not more than 5 business days after receipt of notification.
    - Employer must provide an explanation of discrepancy, time period to contest, and provide the original notice within 7 business days.
    - Employer must provide notification to employee's representative within same time frame.
    - Notification should be by hand if possible, but if not possible, notification must be by mail and email.
- When an employer receives notice of an upcoming inspection by an agency of I-9 forms or other related documents:
    - Employer must provide notice to all employees in all relevant languages within 72 hours of receipt of the notice.
    - Employer must also provide written notice to employees' representatives, when applicable.
    - Notice should include details regarding the conducting agency, the date the notice was received, the nature of the inspection and a copy of the notice. (IDOL is expected to prepare a template for this notification.)
- If during an inspection, a problem is uncovered about a specific employee:
    - Employer must provide written notice to the employee and employee's representative within 5 business days.
    - Notice should be provided in person if possible or by mail and email.
    - Notice should include a full explanation of what was found, the time period for the employee to notify the employer if they plan to contest the finding, the time and date of any upcoming meetings on the topic, and the employee's right to representation.
    - If the employee contests the determination, the employer must notify the employee within 72 hours after receipt of a final determination and provide the original notice within 7 business days.

CLICK HERE FOR SOURCE ARTICLE

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

Prince George's County in MD Expands Criminal Background Check Laws

The Prince George's County Council recently passed an ordinance, the Employment Fairness Act for Returning Citizens, which further restricts an employer's ability to conduct criminal background checks. The ordinance took effect on September 16, 2024.

Employers with *10 or more full-time employees* in the County are now subject to the ordinance, a reduction from the previous threshold of 25 employees.

Under the ordinance, employers are prohibited from doing the following:

- requiring an applicant to disclose on an application the existence of the applicant's arrest or conviction record
- requiring the applicant to disclose *before the conclusion of the first interview* whether the applicant has an arrest or conviction record or has been accused of a crime
- conducting a criminal record check on the applicant or inquiring about whether the applicant has an arrest or conviction record or has been accused of the crime *before the conclusion of the first interview*

Employers are now prohibited from doing the following at *any time*:

- inquiring into or considering convictions of any applicant where the sentence was completed for a nonviolent felony at least 60 months ago or for a misdemeanor where the sentence was completed at least 30 months ago
- inquiring about or considering any arrests that did not result in a conviction (unless the result was probation before judgment)
- inquiring about or considering arrests or convictions for possession of marijuana or cannabis-related paraphernalia if the sentence has been completed
- conducting background checks or investigations that do not conform to these restrictions.

The ordinance also expands the definitions of key terms. An "arrest" now encompasses any apprehension, detention, or custody by law enforcement, even if no charges are brought. A "conviction" now means any guilty verdict or plea, including a plea of nolo contendere. A "nonviolent felony" is any felony that does not meet the state's definition of a violent crime.

Takeaways
Employers with 10 or more full-time employees in Prince George's County should consider whether they are now subject to County limitations on considering criminal background information. Employers should also review these new limitations to ensure their background screening policies are compliant with County standards. Please do not hesitate to reach out for assistance in ensuring your business's hiring processes are consistent with applicable criminal background check laws.

CLICK HERE FOR SOURCE ARTICLE

Just Around the Corner, Iowa's Consumer Privacy Law Taking Effect

Iowa is next up in our series of articles providing in-depth summaries of state consumer privacy laws taking effect across the nation.

On March 28, 2023, Iowa Governor Kim Reynolds (R) signed into law Senate File 262 (the Iowa Consumer Data Protection Act or "IACDPA") which becomes effective on January 1, 2025. The law aligns with other business-friendly state consumer privacy laws, but notably foregoes the requirement of conducting data protection impact assessments, and the IACDPA does not give consumers the right to correct personal data.

For additional resources about state consumer privacy laws, we are including an index at the bottom of this articles with hyperlinks to our blog posts covering laws passed in other states. Please also keep your eye out for our 2024 round-up article that will be published in December as it will be a helpful overview of the full landscape of consumer privacy laws across the United States.

To Whom Does the Iowa Consumer Data Protection Act Apply?
The IACDPA applies to any individual or entity who either conducts business in Iowa or produces products or services that are targeted to the residents of Iowa; and that, during a calendar year either:

- controls or processes personal data of at least 100,000 Iowa residents; or

- controls or processes personal data of at least 25,000 Iowa residents and derives over 50% of its gross revenue from the sale of personal data.

Unlike broader and more onerous state consumer privacy laws, the IACDPA has narrower application to entities that *target* Iowa residents, as opposed to those who merely *provide* services or products to Iowa residents.

The IACDPA applies to personal data collected from a natural person who is a resident of the state and acts in any capacity other than in a commercial or employment context.

Iowa Consumer Data Protection Act Exemptions

In keeping with many other state consumer privacy laws in the country, the IACDPA exempts non-profit organizations, government entities, both public and private higher-ed institutions, and data addressed by sectoral privacy laws such as HIPAA and the Gramm- Leach- Bliley Act. Furthermore, the IACDPA also exempts specific types of data such as business-to-business personal data, data provided in the employment context, consumer credit-reporting data, health records, scientific research data, and information regulated under the federal Family Educational Rights and Privacy Act and Farm Credit Act.

Consumer Rights

Consumers have the following rights under the IACDPA:

- right to confirm whether or not their personal data is processed;
- right to access their personal data;
- right to deletion of their personal data;
- right to obtain a copy of their personal data;
- right to portability of their personal data;
- right to opt-out of the processing of their personal data for purpose of the sale of personal data and targeted advertising, and
- right to opt out of sensitive data processing.

Notably, and unlike more consumer-friendly state privacy laws, Iowa's statute does not include a consumer's right to correct personal data, and instead of allowing consumers to opt-in to sensitive data processing, it requires covered entities to provide consumers with the opportunity to opt out of this form of data processing.

Business Obligations to Consumers

The IACDPA requires covered entities to:

- respond to consumer requests under the IACDPA within 90 days of receipt of such request (and may be extended an additional 45 days when reasonably necessary, depending on number and complexity of requests);
- if the business declines to act on the consumer's request, it must inform the consumer and provide instructions on how to appeal the decision;
- establish a process for consumers to appeal any refusal to take action on a consumer request; and
- within 60 days of receipt of a request for appeal, the business must inform the consumer of any action or inaction in response to the appeal, and if denied, provide the consumer with an online mechanism through which the consumer may reach the Iowa Attorney General to submit a complaint.

Notices to Consumers

Covered entities must provide consumers with a "reasonably accessible, clear and meaningful" privacy notice that includes at a minimum the following:

- the categories of personal data that the business processes;
- the express purposes for which the business is collecting and processing personal data;
- a list of all categories of personal data that a business shares with third parties;
- the categories of third parties with which the business shares personal data; and
- the manner in which consumers can exercise their rights under the IACDPA, including the process for appeals of denials of consumer requests.

As highlighted above, the IACDPA takes another departure from many other state privacy laws and does not require businesses to conduct and document data protection impact assessments in connection with the processing of personal data.

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

Other Business Obligations
Covered entities must (the DO's):

- limit the processing of personal data to only the data that is "adequate, relevant, reasonably necessary, and proportionate" to serve the purposes for which the data is collected and processed;
- establish, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the confidentiality, integrity, and security of the personal data;
- clearly and conspicuously disclose if the business sells consumers' personal data to third parties or engages in targeted advertising; and
- provide consumers an opportunity to opt out from the sale of their personal data to third parties or engaging in targeted advertising.

Covered entities must not (the DON'Ts):

- process consumers' sensitive data without presenting the consumer with clear notice and an opportunity to opt out of such processing; or if the consumer is a child, must process sensitive data in accordance with the federal Children's Online Privacy Protection Act ("COPPA");
    - Sensitive data is defined as a category of personal data that includes "racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, except to the extent such data is used in order to avoid discrimination on the basis of a protected class that would violate a federal or state anti-discrimination law, genetic or biometric data that is processed for the purpose of uniquely identifying a natural person, personal data collected from a known child, and precise geolocation data.
- process the sensitive data concerning a known child without complying with COPPA;
- process personal data in violation of state and federal laws that prohibit unlawful discrimination against a consumer;
- discriminate against consumers who exercise the rights under the IACDPA; and
- require a consumer to create a new account in order to exercise consumer rights (but may require a consumer to use an existing account).

Impact on Vendors/ Data Processors
Subprocessors such as vendors to covered businesses most often will have direct obligations under the IACDPA, such as:

- assisting the covered business with their own compliance obligations;
- make available to the covered business all information in the subprocessor's possession necessary to demonstrate the entity's compliance with the IACDPA;
- ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; and
- at the covered business' direction, delete or return all personal data to it, unless retention is required by law.

Subprocessors must enter into a contract with the covered business that governs how it processes personal data on the covered business' behalf. The IACDPA contains the following requirements that must be included in data processing agreements between the parties:

- instructions for processing personal data;
- the nature and purpose of processing;
- the type of data subject to processing;
- the duration of processing; and
- the rights and duties of both parties.

Enforcement
Like most state consumer privacy laws, the IACDPA does not provide for a private right of action. The IACDPA is exclusively enforced by the Iowa Office of the Attorney General and provides for a 90-day cure period where, prior to bringing an enforcement action, the AG will notify a covered business and grant it an opportunity to cure (if a cure is deemed possible).

Fines and Penalties
The Iowa Attorney General may recover up to $7,500 in civil penalties per violation of the IACDPA.

CLICK HERE FOR SOURCE ARTICLE

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

COURT CASES

Drug Testing in Nuclear Industry – Federal Court of Appeal Confirms the Risk Management Approach to Pre-Placement and Random Alcohol and Drug Testing is Reasonable in the Nuclear Industry

In the long-awaited appeal of *Power Workers' Union v. Canada (Attorney General)*,[i] the Federal Court of Appeal (FCA) upheld pre-placement and random alcohol and drug testing as constitutional and reasonable for safety-critical workers in the nuclear industry. This decision confirms the ability of legislature to include such testing requirements within safety-sensitive industries, and it will hopefully pave the way for more such legislation to help employers in their efforts to maintain workplace safety.

Background facts
In January 2021, the Canadian Nuclear Safety Commission (Commission) imposed the requirement for various forms of alcohol and drug testing as a condition to persons licenced to operate high security, "Class I" nuclear facilities (Licensees). The requirements for reasonable cause, post-incident and follow-up or return-to-duty testing were relatively uncontroversial, but as expected, the requirements for Licensees to (a) randomly test 25% of their safety-critical workforce each year, and (b) undertake pre-placement alcohol and drug testing were immediately challenged by unions representing affected workers. The unions challenged the provisions of REGDOC-2.2.4, Fitness for Duty, Volume II: Managing Alcohol and Drug Use Version 3 (the Regulations) that related to pre-placement and random testing (the Impugned Provisions) on two bases: (1) that the Impugned Provisions breached the rights of affected workers under sections 7, 8 and 15 of the *Canadian Charter of Rights and Freedoms* and were not saved by section 1 of the *Charter*, and (2) alternatively, that the Commission's decision to implement the Regulations was unreasonable on administrative law grounds.

Based on the nature of the grievances, the arbitrator determined that he did not have jurisdiction and, therefore, judicial review proceedings were scheduled with the Federal Court. The Impugned Provisions were stayed pending the outcome of the judicial review. In its decision, the Federal Court rejected all of the challenges and upheld the Regulations, leading to the appeal before the FCA.

Decision
The FCA reviewed the applicable legislative framework and determined that the Commission, which is the sole nuclear regulator, has broad power and authority to subject Licensees to any terms or conditions that it considers necessary for the purposes of carrying-out the *Nuclear Safety and Control Act*. While the Impugned Provisions are contained in a regulatory document rather than an instrument, the FCA found that regulatory documents are frequently used to implement standards and requirements in the nuclear industry. The FCA then reviewed the three *Charter* claims and administrative challenge in turn.

Section 7 Challenge – Life, Liberty and Security of Person
The FCA determined that section 7 is not engaged, agreeing with the Federal Court that, from the point of view of a reasonable person, the relatively non-invasive nature of the seizure permitted by the Impugned Provisions, coupled with the absence of disciplinary consequences resulting from a positive test, does not rise to the level of serious and profound state-imposed psychological stress required to engage section 7 protection.

Section 8 Challenge – Search and Seizure
A section 8 challenge involves a two-step analysis: (1) does the impugned search or seizure interfere with an individual's reasonable expectation of privacy, and (2) if so, is the action reasonable? The FCA reiterated that a flexible approach must be taken, calling for a contextual analysis. Here, the context involves a highly regulated industry, where a "wait and see" approach to safety is not appropriate. Therefore, despite no evidence of impairment being an issue at nuclear sites, there is evidence of gaps in the fitness for duty programs when it comes to addressing alcohol and drug impairment. Filling the gaps is a valid and compelling objective.

When considering reasonable expectations of privacy, the FCA clarified that a "twin subjective/objective enquiry" is required, determining reasonable expectation of privacy in the totality of the circumstances. The FCA followed prior case law in concluding that "safety-critical workers have a diminished expectation of privacy, given the nature of their work and the unique environment in which that work is being performed." The FCA further concluded that the taking of breath, urine

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

or saliva samples are amongst the less intrusive when it comes to bodily searches.

Despite the diminished reasonable expectation of privacy, the affected workers are entitled to protection of section 8, thus requiring an analysis of whether the Impugned Provisions are reasonable. Due to the presumption that searches and seizures without a warrant are unreasonable, the burden shifted to the state to establish reasonableness. The FCA determined that the Impugned Provisions were "authorized by law" and that the authorizing law itself is reasonable. Ultimately, the FCA concluded that the affected workers' interest in being left alone by the government does not outweigh the government's interest in intruding on privacy to advance the goals of limiting risk to national security, the health and safety of persons, and the environment associated with the development, production and use of nuclear energy.

Section 15 Challenge – Equality
The FCA agreed with the Federal Court that the Impugned Provisions create a distinction based on job category, which is not a distinction based on an enumerated or analogous ground of discrimination for the purposes of section 15, nor do the Impugned Provisions create a distinction based on an enumerated or analogous ground due to their alleged impacts on workers suffering from drug dependency. Notably, there is no evidence of drug dependency amongst safety-critical workers to support a claim that a disproportionate number would be affected by the Impugned Provisions. In any event, the FCA concluded that "there is nothing arbitrary in removing such worker from safety-critical duties until that worker is deemed fit for duty."

Because the section 7, 8, and 15 challenges were not successful, the FCA did not undergo a section 1 analysis.

Administrative challenge
Under this challenge, the appellants argued that: (1) there were inadequate reasons for why the Commission approved the Regulations, and (2) there was fettered discretion. The FCA dismissed both arguments. With respect to the adequacy of reasons, the FCA found that the Commission was entitled to rely on the work done by its staff throughout the 10-year consultation process to support its decision, and that the Commission was actively engaged with the staff throughout the consultation process. With respect to fettered discretion, the FCA, again, reiterated that the Commission has the power to set conditions for Licensees, and the fact that the public had been invited to participate in the consultation process did not impair the authority to adopt and implement the Regulations.

Having addressed both the *Charter* challenge and the administrative challenge, the FCA dismissed the Appeal and upheld the requirement for pre-placement and random alcohol and drug testing of safety-critical workers in the nuclear industry.

Effect and takeaways
On its face, this decision carries little authority beyond the nuclear industry. The FCA (and Federal Court) made it clear that its decision was based on the "unique context" of the nuclear industry where incidents may result in devastating and long-lasting impacts on the community and the environment, noting that the nuclear industry is "unlike any other inherently dangerous industries in Canada."

However, despite being unable to rely on the decision as authority for the implementation of pre-placement or random testing in all inherently dangerous industries, this decision is undoubtedly impactful for its commentary on the expectation of privacy in safety-sensitive positions, the invasiveness (or lack thereof) of testing methods, and the role of legislation in the implementation of requirements for alcohol and drug testing within regulated industries. The FCA's practical, pre-emptive approach to safety in an inherently dangerous industry is a breath of fresh air for employers fighting to balance safety obligations with privacy rights, but its applicability across other safety-sensitive industries is yet to be seen.

CLICK HERE FOR SOURCE ARTICLE

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

INTERNATIONAL DEVELOPMENTS

Portugal - The Age of Salary Transparency

The issue of equal treatment between men and women in the workplace is nothing new; however, it gained new impetus with the publication, in May 2023, of Directive (EU) 2023/970.

Although published and in force for over a year now, this Directive does not seem to have received due attention by many organisations in Portugal.

In fact, according to recent studies on pay transparency in Portugal, although the majority of the companies covered by the studies stated that they were working on the issue of pay transparency, the truth is that almost half revealed that they were still unaware of the Directive and its implications.

The fact that the transposition deadline is set for June 2026 may be contributing to organisations' lack of sense of urgency in anticipating the Directive's implications.

It is true that Portugal already has in place Law 60/2018, of 21 August, the purpose of which is to promote equal pay for women and men for equal work or work of equal value, notably by imposing on companies the obligation to establish a transparent remuneration policy, compliance with which has recently been widely scrutinised by the Authority for Working Conditions (*Autoridade para as Condições do Trabalho*, or "ACT"), as well as Law 62/2017, of 1 August, establishing a regime of balanced representation between women and men in the management and supervisory bodies of public sector companies and listed companies, and Law 26/2019, of 28 March, establishing a regime of balanced representation between women and men in Public Administration executive positions and governing bodies.

However, according to the latest data collected by the Portuguese Gender Pay Gap Barometer, published by the Strategy and Planning Office of the Ministry of Labour, Solidarity and Social Security, for the year 2022, a slight increase was registered in the gender pay gap compared to 2021 – a trend that had been reversed since 2010.

The new Directive imposes a set of obligations on companies in terms of pay transparency, which, once transposed, will entail a considerable change to the applicable framework (in both the public and private sectors).

What are the Directive's main obligations in terms of pay transparency?

Job seekers
(i) Job seekers will be entitled to receive information about the starting salary or salary range for the position they are applying for, before the job interview (e.g., in the job advert).
(ii) In addition, candidates should not be asked how much they earn or earned in their current or previous job, thus putting an end to interview questions about salary expectations.
(iii) Job adverts and job titles shall be gender neutral, and recruitment processes shall be conducted in a non-discriminatory way.

Workers
(i) Workers shall have access to the criteria used to determine their pay, pay levels, and career progression. These criteria shall be objective and gender neutral.
(ii) Upon written request, workers shall have access to information on their individual pay level and the average pay levels, broken down by sex, for categories of workers performing the same work as them or work of equal value to theirs.
(iii) Workers cannot be prevented from disclosing their pay in order to guarantee the effective application of the principle of equal pay, and it will no longer be possible to include a clause in the employment contract subjecting such information to a duty of confidentiality.
(iv) Workers who consider themselves wronged as a result of the violation of a right or obligation related to the principle of equal pay will be entitled to claim compensation for the damage suffered or full reparation, with the burden of proving that there was no violation being placed on the employer whenever workers present facts that give rise to a presumption of discrimination.

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

Employers

(i) Employers will be obliged to inform all workers, on a yearly basis, of their right to request and receive pay-related information.

(ii) Employers with 100 or more employees will now have to periodically report to the ACT information on pay disparities existing between female and male employees.

In this regard, we highlight that Law 60/2018 already provides a broader subjective scope, extending the need to implement a pay gap assessment plan to employers with more than 50 workers. As such, we anticipate the maintenance of this limit as possible for the purposes of the obligations arising from the Directive.

(iii) If the information reported reveals a gender pay gap greater than 5%, employers will have to provide the corresponding justification in an objective and gender-neutral way.

(iv) If this justification is not provided or the disparity is not corrected within six months of the date on which the pay gap information was communicated, employers will be subject to a joint pay assessment, carried out in cooperation with the representatives of the relevant employees, with a view to identifying, correcting and preventing pay gaps between female and male workers that are not justified on the basis of objective, gender-neutral criteria.

(v) In addition to the possible payment of compensation to workers, other sanctions, such as fines, may be imposed on organizations in the event of non-compliance with pay transparency obligations.

What should organizations start doing in terms of pay transparency?

Although the deadline for transposition of the Directive is still more than a year and a half away and the exact terms of its implementation in Portugal are not yet known, organizations should start preparing and implementing measures to promote pay transparency, such as:

- Implementation and/or revision of the transparent remuneration policy in force;
- Provision of training on pay discrimination;
- Identification of existing job positions and critical analysis of their various components in order to determine any pay differences between jobs of equal value;
- Drawing up action plans for equal pay;
- Review of pay and career progression structures;
- Review of the information included in recruitment and selection processes;
- Review of employment contracts.

Organisations should view the measures arising from the Directive as a business opportunity, considering that by eliminating discriminatory factors they not only make themselves more attractive, but also encourage the building of a more diverse workforce, with all the benefits this brings. In this way, organisations' anticipation of the measures outlined will certainly prove a competitive advantage.

In sum, the anticipation of these measures in line with the guidelines set forth by the Pay Transparency Directive is not only a prudent management goal but should be assumed as a strategic priority for organisations given the impact that failure to do so will have on their business, costs, and people management.

CLICK HERE FOR SOURCE ARTICLE

Sex offenders will not be allowed to change their names in Ontario, solicitor general says

Offenders would be required to disclose email, social media accounts under proposed legal changes

Ontario plans to ban registered sex offenders from changing their names.

Solicitor General Michael Kerzner says those who are on the provincial sex offender registry will no longer be allowed to legally change their name once new legislation is passed.

Kerzner says his government's planned changes to Christopher's Law would also require registered sex offenders to disclose their email and social media accounts, and report any changes to their usernames.

Offenders would also face stricter travel rules, including a requirement to report new passports or driver's licences.

Christopher's Law is named for 11-year-old Christopher Stephenson, who was murdered by a convicted sex offender on Father's Day in 1988.

His father, Jim Stephenson, says the changes will help police solve sex crimes and protect vulnerable children.

CLICK HERE FOR SOURCE ARTICLE

Malaysia: Why background checks are crucial in modern hiring

Datuk Dr Syed Hussain Syed Husman, the president of the Malaysian Employers Federation, recently weighed in on the matter, stressing the need for more robust background checks, particularly in industries such as food and beverage, where safety and hygiene are non-negotiable. He argued that such precautions not only safeguard workplace environments but also bolster consumer trust.

“Clients feel reassured knowing that the individuals they interact with have been properly vetted,” he said, as first reported by The Sun. “To prevent untoward incidents, a comprehensive hiring process that includes multiple layers of verification is crucial.”

The hiring process is akin to building a fortress – layer by layer. For Syed Hussain, it should include detailed reference checks, psychological evaluations, and regular updates to hiring policies.

These measures act as the first line of defence against individuals who might engage in misconduct or jeopardise workplace harmony.

Also Read: 1 in 3 Malaysians threatened by generative AI: report

Lessons for employers
Highlighting the challenges of vetting entry-level and part-time workers, Syed Hussain pointed to the food and beverage sector as a cautionary tale.

“Employers need to have clear policies for dealing with cases of concealed identity or false information to safeguard themselves,” he said.

“Once a person is hired, it will be a tedious process to terminate the employment, which includes conducting a domestic inquiry to take the necessary disciplinary action.”

Younger employees, he noted, often seek attention through social media antics, which can inadvertently harm their employers.

For businesses, adopting clear policies to address cases of falsified information or concealed identities is crucial. Terminating an employee with questionable conduct, he cautioned, could be a long and bureaucratic process involving disciplinary inquiries.

However, even as businesses ramp up scrutiny, they must tread carefully to ensure compliance with the Personal Data Protection Act. Transparency and respect for candidates’ privacy rights remain essential, creating a fine line between due diligence and overreach.

Exposure on social media
The trickiest place to check for reputational blunders, of course, is social media. As hiring becomes more complex, businesses must see background checks not as an optional step but as a cornerstone of their recruitment strategy. A lapse in due diligence can be costly, turning what seemed like a perfect hire into a PR nightmare.

“A social media background check uses the candidate’s own social media handles and scans their profiles, as well as their activities across social media platforms. Everything from comments to likes, shares, and posts, are assessed. It then produces a result that lets you know how those individuals fit within your company’s culture, value, and more,” explained Robert

Stewart, chief revenue officer at Triton Canada, a specialist in background checks.

“As an HR leader/executive the cost to you to recruit candidates that do not align with your organisational values is far higher than the negligible cost associated with giving your team the ability to obtain social media background checks on viable candidates,” Steward said.

Discriminating against candidates

With advanced tools now at their disposal, business and HR leaders can easily develop a more complete view of a candidate’s online reputation.

“While the benefits of social media screening are clear, the practice is not without its pitfalls. One of the primary concerns is the potential for bias and discrimination,” said Linda Wolters, a strategic account manager from background screening solutions provider Data Facts.

“Social media profiles often contain information related to a candidate’s age, race, gender, religion, and other protected characteristics. If this information influences hiring decisions, it can lead to discriminatory practices, whether intentional or not.”

“As with any background screening service, it is required that you obtain consent from candidates before conducting social media checks. This can help mitigate privacy concerns and ensure transparency,” Wolters said.

“Only consider information that is directly relevant to the job and the candidate’s ability to perform their duties. Avoid making decisions based on personal characteristics or opinions.”

In an era where reputations are built and broken online, employers must treat hiring as a delicate balancing act. It’s about walking the tightrope between being vigilant and being respectful of candidates’ rights, ensuring that the workplace remains a safe and trustworthy environment for all.

After all, a single bad apple can spoil the bunch, but a well-maintained hiring process can keep the entire orchard thriving.

CLICK HERE FOR SOURCE ARTICLE

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

MISCELLANEOUS DEVELOPMENTS

Amendments to Illinois Human Rights Act to Take Effect in 2025

Amendments to the Illinois Human Rights Act ("IHRA"), which will go into effect on January 1, 2025, will prohibit harassment and discrimination against employees based on their reproductive health decisions and family responsibilities, and will prohibit retaliation against employees who report or oppose harassment or discrimination based on those newly defined protected characteristics. Employees will also have two (2) years after an alleged unlawful act to file a charge of discrimination. Employers should be mindful of these changes and adjust their policies and practices as appropriate.

Reproductive Health Decisions
Effective January 1, 2025, employers will be prohibited from discriminating against and harassing employees due to their "reproductive health decisions," meaning decisions regarding the use of contraception, fertility or sterilization care, assisted reproductive technologies, miscarriage management care, health care related to the continuation or termination of pregnancy, and prenatal, intranatal or postnatal care.

Family Responsibilities
The new amendments will also prohibit harassment and discrimination against employees based on "family responsibilities," meaning an individual's actual or perceived provision of personal care to a family member. The term "personal care" is defined broadly to include activities to ensure that a family member's basic medical, hygiene, nutritional or safety needs are met, or to provide transportation to medical appointments for a family member who is unable to meet those needs himself or herself. "Personal care" also includes being physically present to provide emotional support to a family member with a serious health condition who is receiving inpatient or home care. A "family member" includes an employee's child, stepchild, spouse, domestic partner, sibling, parent, mother-in-law, father-in-law, grandchild, grandparent or stepparent.

Of note, the amendment will not require employers to make modifications to their reasonable workplace policies to accommodate an employee's family responsibilities. This means, for example, that an employer does not need to provide an employee with time off, a flexible work schedule or a work-from-home arrangement to provide personal care to a sick family member; however, other laws, such as the federal Family Medical Leave Act or the Illinois Paid Leave for All Workers Act may apply. Moreover, the amendment clarifies that nothing in the IHRA prevents an employer from taking adverse action or otherwise enforcing reasonable workplace rules or policies related to leave, scheduling, productivity, absenteeism, work performance or others against an employee with family responsibilities, provided those policies are applied consistently with the law.

Statute of Limitations Extended
Significantly, the new IHRA amendments will also extend the time an employee has to file a charge with the Illinois Department of Human Rights from 300 days to two (2) years from the date the alleged violation occurred.

Next Steps for Employers
Illinois employers should prepare for these changes to the IHRA and consider updating their employee handbooks and training their front-line managers to understand the types of conduct that are protected.

CLICK HERE FOR SOURCE ARTICLE

SB 1137 Expands California's Civil Rights Laws Prohibiting Discrimination Based on "Any Combination Of" Protected Characteristics, A.K.A. "Intersectionality"

On September 27, 2024, Governor Newsom signed Senate Bill ("SB") 1137 which amends Civil Code section 51, Education Code sections 200 and 210.2, and Government Code sections 12920 and 12926, relating to discrimination. The provisions of SB 1137 are stated to be declaratory of existing law, and therefore went into effect on September 27, 2024.

In passing SB 1137, the Legislature included in its declaration:

It is the intent of the Legislature to hereby recognize the concept of intersectionality in California's civil rights laws.

Intersectionality is an analytical framework that sets forth that different forms of inequality operate together, exacerbate each other, and can result in amplified forms of prejudice and harm. The framework and term "intersectionality," coined and popularized by legal scholar Professor Kimberlé Williams Crenshaw, captures the unique, interlocking forms of discrimination and harassment experienced by individuals in the workplace and throughout society, particularly Black women, as compared to Black men and White women.

The Legislature recognizes that where two or more bases for discrimination or harassment exist, they cannot be neatly reduced to distinct components. The attempt to bisect a person's identity at the combination of multiple protected characteristics often distorts or ignores the particular nature of their experiences. When a person claims multiple bases for discrimination or harassment, it may be necessary to determine whether the discrimination or harassment occurred on the basis of a combination of those factors, not just based on any one protected characteristic by itself. In this regard, the Legislature affirms the decision of the Ninth Circuit Court of Appeals in *Lam v. University of Hawai'i* (9th Cir. 1994) 40 F.3d 1551.

Even prior to the passage of SB 1137, all persons in public schools were protected from discrimination on the basis of their protected characteristics. SB 1137 expands existing nondiscrimination mandates to also prohibit discrimination based on "any combination of" protected characteristics under the law. SB 1137 also expands the operative definition of "race" to include discrimination complaints based on "traits associated with race, including, but not limited to, hair texture and protected hairstyles." Under the amendments of SB 1137, a group or class of individuals may now file a single complaint "alleging a pattern or practice" of discriminatory conduct based on a protected characteristic.

In response to SB 1137, Local Educational Agencies ("LEA") should be sure to update their policies related to complaints of discrimination to reflect that discrimination is prohibited not only based on one specific protected trait, but also on the combination of any one or more protected characteristics. Although these protections are not new, LEAs should be sure to address allegations that discrimination was based on the combination of two or more protected characteristics when investigating complaints of discrimination, and account for any potential impact of the combination on investigatory findings.

CLICK HERE FOR SOURCE ARTICLE

California Has Expanded Workplace Protections for Victims of Crimes

California Governor Gavin Newsom signed into law Assembly Bill No. 2499, which shall take effect on January 1, 2025, and expands employee protections for taking time off work if an employee or their family member is a victim of certain crimes or violent acts. The majority of the changes only apply to those employers with 25 or more employees.

Employers With 25 Or More Employees

For employers with 25 or more employees, employees may take leave for the following reasons when either the employee or their family member is the victim of a qualifying act of violence:

- To obtain or attempt to obtain legal relief for the family member, such as a restraining order or other injunctive relief.
- To seek, obtain, or assist a family member seeking or obtaining, services from a domestic violence shelter, rape crisis center, or victim services organization or agency.
- To seek, obtain, or assist a family member seeking or obtaining, psychological counseling or mental health services.
- To participate in safety planning or take other actions to increase safety.
- To relocate or engage in the process of securing a new residence. (If the employee's family member is a victim who is not deceased as a result of the crime, and the employee is not a victim, the employer may limit the leave they take for this reason to five days.)
- To care for a family member who is recovering from injuries caused by a qualifying act of violence.
- To seek, obtain, or assist a family member seeking or obtaining, civil or criminal legal services.
- To prepare for, participate in, or attend any civil, administrative, or criminal legal proceeding.
- To seek, obtain, or provide childcare or care of a dependent adult if the care is necessary to ensure the safety of the child or dependent adult.

"Qualifying act of violence" includes domestic violence, sexual assault, stalking, acts that cause bodily injury or death, having a weapon drawn or brandished at the individual, and/or experiencing force or threat of force, which could cause physical injury or death. This definition applies regardless of whether anyone is arrested for, prosecuted for, or convicted of committing any crime.

Employers can limit the total leave time taken for these reasons to twelve weeks, unless the employee's family member is a victim (who is not deceased as a result of crime and the employee is not a victim) in which case, leave can be limited to ten days.

Employees may now use paid sick leave in addition to vacation, personal leave, and other paid time off for all the protected time off referenced above. Employers may require this leave to run concurrently with any leave entitlements under the Federal Family and Medical Leave Act or the California Family Rights Act if the employee is eligible for such leave(s).

All Employers
All employers must reasonably accommodate employees who request an accommodation for the safety of themselves at work if their family member (rather than the employee) is a victim of a qualifying act of violence. Permission to carry a telephone at work is identified as a possible reasonable accommodation.

Employers must now inform their employees of the rights to leave for victims of crime. The notice of rights must be in writing and shall be provided to new employees upon hire, to all employees annually, at any time upon request, and at any time an employee notifies the employer that the employee or their family is a victim. The California Civil Rights Division is developing an optional form for employers' use that complies with the notice requirements.

CLICK HERE FOR SOURCE ARTICLE

Updates to sex offender act help agencies share key details

For the first time last January, the RCMP helped stop a convicted child sex offender from entering another country. The move was possible thanks to updates to the act governing sex offenders — and good collaboration.

One day before the scheduled flight departed from Toronto to Sosua Bay, Dominican Republic, a known destination for transnational child sex offenders, officers at the National Sex Offender Registry (NSOR) and High Risk Sex Offender Program (HRSOP) determined the man was a high risk to reoffend, says the officer in charge of the unit, RCMP Staff Sergeant Alain Gagnon.

In an effort to keep kids overseas safe, they notified the Dominican Republic authorities.

Gagnon says that when the offender touched down in the Dominican Republic, he was denied entry into the country and returned to Canada on the same plane.

"They could have just said 'Thank you, let the guy come in' or they could have watched him to see if he stays where he said he would be staying," says Corporal David Elliott, who oversaw the offender's risk assessment. "But, thankfully, they accepted our assessment."

Elliott is in charge of operations at HRSOP. The program was created in 2016 to address amendments to the *National Sex Offender Information Registration Act*.

The act helps police prevent and investigate sex crimes by requiring convicted sex offenders to provide certain information to police at least once a year, and to be added to the sex offender registry.

Registry rules
As of January 2019, there are more than 51,000 registered sex offenders in the database, according to the latest numbers gathered by the RCMP, which maintains the registry. Of those, approximately 73 per cent are child sex offenders.

Once an offender makes the registry, they're on it for life. Depending on their sentence, they must check in with police in

person at least once a year for either 10 years, 20 years or life. Up to 80 pieces of information are entered into a database that's available to Canadian and international law enforcement agencies.

Under the amended legislation, registered child sex offenders must also report their driver's licence and passport information, and travel plans. Failing to comply could mean going back to prison.

"If they're not reporting or reporting last minute, it's a red flag for us because it shows a mindset and indicates risk," says Elliott.

Thanks to the updates to the act, if the unit determines an offender is high risk they may now share the information with their partner agencies including other police services — in Canada or abroad — and the Canada Border Services Agency (CBSA).

High-risk travellers
Chad Barter is an intelligence officer with the CBSA. For the past two years, he's been embedded with the RCMP in Ottawa, giving investigators relevant traveller information upon request.
As part of his partnership with the RCMP, Barter may disclose a myriad of information that's normally protected under the *Privacy Act*. It includes air travel history, flight seat number, weight and number of luggage, hotel reservations and possible travel associates.

In the case from January, Barter discovered that the offender frequently travelled to child sexual exploitation hotspots.
This, combined with the results of the recidivism risk assessment, was critical in Elliott's decision to flag him as high-risk.
At the request of the RCMP, Barter created an electronic message, called a lookout, which shows up on screen when someone goes through customs upon re-entering Canada. Each time, they will be taken to a room for questioning. Their belongings, including electronics, will also be searched for child exploitation images or other indicators of illegal activities while they were overseas, says Barter.

"If they operate anything like Canada, he'll never enter the Dominican Republic again," says Barter.

With between 2,500 and 3,500 new names added to the registry each year, Gagnon says it's all the more important to continue working with partners, such as the RCMP's National Child Exploitation Coordination Centre, to keep the registry accurate and up to date for officers investigating sex crimes.

"This is one of the most rewarding jobs I've had in my 29 years in the RCMP," says Gagnon. "What we do makes a real difference."

CLICK HERE FOR SOURCE ARTICLE

The Data Protection Legal Framework in Chile

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

In general, there is no special data protection authority in Chile; data protection is overseen and addressed by general courts with general powers. A summary procedure is established by law if the person responsible for the personal data registry or bank fails to respond to a request for access, modification, elimination or blocking of personal data within two business days, or refuses a request on grounds other than the security of the nation or the national interest.
However, other entities have powers in matters of personal data protection, the main ones being the following.

The National Consumer Service
The National Consumer Service (SERNAC) is the control body on matters of personal data protection in the context of consumer relations, until a specialised data protection agency is formed. SERNAC does not have sanctioning powers, although it can exercise its powers to supervise, inspect, investigate, file individual or class actions, and issue interpretative circulars that are mandatory for SERNAC officials when applying the regulation and the Law (eg, at the time of audit).

Among the circulars issued by SERNAC, the main ones are: an interpretative circular on good practices in electronic commerce; an interpretative circular on the criteria of equity in the stipulations in standard form contracts referring to the collection and processing of the personal data of consumers (eg, terms and conditions of use; end user licence agreements etc); and an interpretative circular on consumer protection against the use of artificial intelligence systems.

The Council for Transparency
In the public sector, the Council for Transparency is responsible for ensuring compliance with Law No. 19628 by the organs of the state administration. The Council has issued the Recommendations on Protection of Personal Data by the Organs of the State Administration, the Guide on Protection of Personal Data for Public Institutions (2021), and Resolution No. 489/2022, which approved the Procedure for Processing Requests for the exercise of ARCO (access, rectification, cancellation and objection) rights made before the Council for Transparency.

The Financial Market Commission
The Financial Market Commission (CMF) is the control body in the financial sector and has supervisory powers on matters of personal data protection, information security and cybersecurity. Thus, financial institutions must have an internal policy on the security and management of debtor information (PISMID), which must follow international principles and best practices on personal data processing. In addition, the CMF should dictate the cybersecurity and personal data protection standards that financial institutions participating in the future Open Banking System must comply with. The Open Banking System is regulated by the recently approved Law No. 21521, known as the Fintech Law. Finally, according to the Bill on personal data protection (Bill No. 11.144-07), which is currently being discussed in the National Congress, the planned future agency regulating data protection in Chile will be an independent Personal Data Protection Agency.

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

Currently, there is no data protection authority in Chile. A bill has been discussed in Congress that will reform the whole data protection environment in the country and will create the first data protection authority in Chile.

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

Yes. Breaches of data protection caused by improper processing of data may eventually lead to fines determined by the Law, ranging from 65,443 Chilean pesos to 654,430 Chilean pesos, or from 654,430 Chilean pesos to 3,272,150 Chilean pesos. Fines are determined through a summary proceeding.

The Law establishes a general rule under which both non-monetary and monetary damages that result from wilful misconduct or negligence in the processing of personal data shall be compensated. In those cases, the amount of compensation shall be established reasonably by a civil judge, considering the circumstances of the case and the relevance of the facts.

The Bill on the protection of personal data, on the other hand, proposes a list of minor, serious and very serious infractions, and fines that can reach 654.43 million Chilean pesos and, in the case of companies, a fine of up to the amount equivalent to 4 per cent of the annual income from sales and services and other activities of the line of business during the last calendar year, with a maximum of 1.308 billion Chilean pesos, depending on the seriousness of the infraction.

Scope

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

Law No. 19,628 on Privacy Protection (the Law) applies to both private and public sector organisations and agencies. However, regarding public sector organisations, there are some special rules for the consent of the subject (ie, personal data about sentences for felonies, administrative sanctions or disciplinary failures and the records of personal data banks in government agencies).

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

The Data Protection Law does not cover interception of communications or monitoring and surveillance of individuals. Both matters are regulated by:

- Law No. 21459 (the Computer Crime Law);
- article 161-A, 369-ter, 411-octies of the Penal Code; and
- articles 222 to 226 of the Criminal Code of Procedure.

The Data Protection Law does cover electronic marketing, in the sense of establishing that no authorisation is required to make electronic marketing when the information comes from sources available to the public (registries or collection of personal data, public or private, with unrestricted or unreserved access to the requesters).

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

Numerous laws address privacy issues, for example:

- Law No. 21459 (the Computer Crime Law);
- Law No. 21663 (the Cybersecurity Framework Law);
- article 161-A, 369-ter, 411-octies of the Penal Code;
- articles 222 to 226 of the Criminal Code of Procedure;
- Law No. 20584, which contains provisions regarding the privacy of medical records along with Law No. 19,628, which contains provisions stipulating that a doctor's prescriptions and laboratory analyses or exams and services related to health are confidential;
- Law No. 19496, which contains provisions regarding credit information along with the same Law No. 19,628, which contains provisions about personal data related to obligations of an economic, financial, banking or commercial character;
- Law No. 18290, which contains provisions regarding the privacy of a driver's information;
- Law No. 19799 regarding electronic signatures, which contains the right to privacy of the holder of an electronic signature;
- article 154-bis of the Labour Code, which establishes that the employer shall keep confidential all the information and private data of the worker to which he or she has to access on the occasion of the employment relationship. Also, article 5 of the Labour Code establishes that the exercise of powers granted to the employer by law is limited by respect for the constitutional guarantees of the workers, especially when they may affect their privacy, private life or honour;
- Law No. 21521, known as the Fintech Law, which 'promotes competition and financial inclusion through innovation and technology in the provision of financial services';
- Law No. 21541, which authorises health providers to perform health care through telemedicine;
- Law No. 21398, or the Pro-Consumer Law, which granted the National Consumer Service the status of a control body on matters of personal data protection in the context of consumer relations until the establishment of a specialised body in the protection of personal data;
- Decree No. 6/2021, which approves the Electronic Commerce Regulation; and
- Decree No. 6/2022, which approves the Regulation on actions related to remote health care.

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

The Law regulates the following categories or types of personal information (PI):

- personal data: those related to any information concerning identified or identifiable natural persons;

- sensitive personal data: those related to the physical or moral characteristics of persons or to facts or circumstances of their private or intimate life, such as personal habits, racial origin, ideologies and political opinions, beliefs or religious convictions, conditions of physical or mental health, and sex life; and
- personal data relating to obligations of an economic, financial, banking or commercial nature.

On the other hand, the Bill on the protection of personal data would add other categories of PI to the Law, such as geolocation data, biometric data, health data, and personal data of children and adolescents, among others.

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

The Law does not contain an explicit provision in this respect; however, any use of the data will require the consent or authorisation of the holder or subject of the personal data, if it is not subject to the exceptions mentioned in this chapter (transfer is a kind of personal data processing; thus, all the data privacy rules shall apply, including the consent requirement).
For its part, the Bill on the protection of personal data would amend the Law and, therefore, would add grounds for extraterritorial application of the Law.

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

Yes, all processing of PI is covered. 'Data processing' is broadly defined in the Law as any operation or set of technical operations or procedures, automated or not, that make it possible to collect, store, record, organise, prepare, select, extract, match, interconnect, dissociate, communicate, assign, transfer, transmit or cancel personal data, or use it in any form. There is no distinction made between those who control or own PI and those who provide PI processing services to owners. The Law only refers to the 'person responsible for a data registry or a bank', which means any private legal entity or individual, or government agency, that has the authority to implement the decisions related to the processing of personal data. Therefore, there are no different duties for owners, controllers or processors. However, government agencies can only process data regarding matters within their respective legal authority and subject to the rules set out in the Law.

On the other hand, the Bill on personal data protection, amending the Law, distinguishes between data subjects, data controllers and data processors, and assigns specific rights, obligations, duties or tasks to each of them.

CLICK HERE FOR SOURCE ARTICLE

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net