Monthly Newsletter: March 2024

FEDERAL DEVELOPMENTS

Biden Administration Issues Executive Order to Protect Sensitive Personal Data

The White House recently issued an executive order that restricts cross-border transfers of personal data from the United States to "countries of concern."

President Biden also urged Congress to pass comprehensive privacy legislation, especially to protect children.

Key points:

- Focus is on sensitive data, including genomic data, biometric data, personal health data, geolocation data and financial data.
- Concerns are with the sharing and re-sharing of the data through data brokers, such that it ends up in the hands of foreign intelligence services, militaries or companies controlled by foreign government.
- S. Department of State will issue regulations.
- S. Department of Justice will also issue regulations.
- DOJ and U.S. Department of Homeland Security will issue security standards to prevent access by countries of concern to Americans' data through other commercial means, such as data available via investment, vendor and employment relationships.
- S. Department of Health and Human Services (HHS), U.S. Department of Defense and U.S. Department of Veterans Affairs will work to ensure that federal grants, contracts and awards are not used to facilitate access to Americans' sensitive health data by countries of concern, including via companies located in the United States.
- The above should not stop the flow of information necessary for financial services activities. It also should not impose measures aimed at a broader decoupling of the substantial consumer, economic, scientific and trade relationships that the United States has with other countries.

Click Here for the Original Article

FTC Post: Questions About Tenant Background Checks? New Guidance Can Help

If you're looking for a new place to live — or about to renew your lease — a landlord may run a tenant background check to decide whether to rent to you or not. The tenant background check process can be confusing, and renters often don't know how the process works or what to do if something goes wrong. The FTC, Consumer Financial Protection Bureau, Department of Housing & Urban Development (HUD), and Department of Justice have put out a new publication to help renters navigate the screening process.

Tenant background checks are usually compiled by tenant background check companies that put together a report on you and the people you live with. The tenant background check report — sometimes called a resident or tenant screening report — may have information about whether you pay your bills, if you've been evicted or have a criminal record, and more. But it's often hard for you to know exactly what's in your report before you apply and how a landlord might be using it. According to a CFPB study, many renters pay for this kind of background check but they don't get to see the reports that landlords use, which may include mistakes like information that's outdated, misleading, or that belongs to someone else.

The new publication tells you how tenant background checks work, what kinds of background information a landlord might receive about you, how to respond if you think that information is wrong, and your rights under federal laws — including laws related to tenant background checks and those that outlaw discrimination. For example, if the landlord makes a negative decision about your application because of your tenant background check report, you have the right to request a free copy of your report from the tenant background check company. You also have the right to dispute mistakes on your tenant background check report. Because the tenant screening process can be confusing, the FTC has another new article that goes into more detail about how to deal with mistakes in your tenant background check report.

To learn more, check out Tenant Background Checks and Your Rights and Disputing Errors on Your Tenant Background Check Report.

Click Here for the Original Article

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

County of Los Angeles Enacts a Sweeping Fair Chance Ordinance for the Unincorporated Areas of the County that Far Exceeds Federal and California Law

In 2016, the City of Los Angeles enacted a detailed fair chance hiring ordinance. A comprehensive statewide law followed in 2017. Soon, employers with jobs located in the unincorporated areas of the County of Los Angeles must navigate yet another layer of burdensome regulations based on the County's new fair chance hiring ordinance. The ordinance, which imposes obligations *well beyond* existing federal and state law, and which extends to contractor and freelance workers, will take effect on September 3, 2024. It adds to the many and considerable headaches employers already have regarding criminal background checks in California.

The summary below is not exhaustive. It does not canvass all of the particulars of the ordinance, including for employers such as banks, which have restrictions on hiring applicants with criminal records. Additionally, in light of recent and significant *delays* in obtaining criminal background checks in the County, covered employers with jobs located in the unincorporated areas of the County should be aware that the ordinance restricts employers from taking adverse action, such as rescinding a conditional job offer, unless the employer can show "undue burden" on its operations from continuing to hold the job open and it has waited at least 10 business days from initially requesting the background report. Specific notice requirements will also apply in this circumstance.

Coverage

The ordinance protects "Applicants." "Applicant" means an individual who is seeking "employment" with an "employer." Employees seeking promotions are also "applicants." "Employee" means any individual whose job involves performing at least two hours of work on average each week within the unincorporated areas of the County.

The ordinance applies to any "employer" that is located or doing business in the unincorporated areas of Los Angeles County and employs five or more employees *regardless of location*. "Employer" includes job placement, temporary agencies, referral agencies and other employment agencies as well as non-profit organizations. "Employer" also includes any entity that evaluates an applicant's or employee's criminal history on behalf of an employer, or acts as an agent of an employer, directly or indirectly, in evaluating an applicant's or employee's criminal history.

Importantly, the ordinance defines "employment" broadly, including contract work. "Employment" means any occupation, vocation, job, or work, including but not limited to temporary or seasonal work, part-time work, contracted work, contingent work, work on commission, and work through the services of a temporary or other employment agency, including non-profit organizations, or any form of vocational or educational training with or without pay. Employment also means work or services provided pursuant to a contract for an employer in furtherance of an employer's business enterprise. The physical location of the employment must be within the unincorporated areas of Los Angeles County, including when a person is working remotely, teleworking, or telecommuting from a location within the unincorporated areas of the County.

Mandatory Requirements for Job Postings and Like Materials

The ordinance prohibits any language in job postings that may deter job applicants from applying (*e.g.*, "No felons"). But it is not just prohibitory. All job solicitations, bulletins, postings, announcements, and advertisements must include language stating that qualified applicants with arrest or conviction records will be considered for employment in accordance with the ordinance and state law. Further, employers that condition job offers on a criminal background check must include in all such materials a list of all "material job duties" of the specific job position for which the employer "reasonably believes" criminal history may have a "direct, adverse, and negative relationship," potentially resulting in the withdrawal of the conditional job offer.

Mandatory Posting Requirements

Employers must post notice of the ordinance at every workplace. Employers also must post the notice on webpages frequently visited by their employees or applicants. Unionized employers must provide copies of the notice to the unions. A form of notice supposedly will be made available by the County of Los Angeles Department of Consumer and Business Affairs (DCBA) before the time the ordinance takes effect.

Unlawful Practices

The ordinance broadly prohibits employers from inquiring into or considering an applicant's criminal history before first extending a conditional job offer. The ordinance also prohibits inquiring into information that already is off-limits based on state law, including Labor Code section 432.7 (which governs records of arrest, including pending charges) and Labor Code section 432.8 (which pertains to certain marijuana-related convictions).

Significantly, even after extending a conditional job offer, employers may not ask candidates directly about their criminal history. Employers may do so, but not until they *first* receive the criminal background check. This is a crucial sequencing restriction on the events in the screening process.

Importantly, the ordinance also restricts the scope of questions about criminal history to *seven years* from the date of disposition, with exceptions for certain roles (*e.g.*, roles that require interacting with minors or dependent adults, etc.). Questions about non-criminal infractions are also prohibited, except for driving-related infractions for jobs requiring some driving for work. These limitations exceed the restrictions in the state law.

Considering Criminal History and Taking Adverse Action

The ordinance mandates a notice to applicants before inquiring into their criminal history. Employers must provide the notice when extending the conditional job offer. The notice must indicate the offer is contingent on passing the criminal history review and a specific statement of "good cause" to review such information. It is not enough for the employer to merely state it reviews such information out of generalized "safety concerns." More particularized information is required. If the employer also intends to review information beyond criminal history, such as employment and education history, the notice must provide a complete list.

The ordinance also requires a documented, written individualized assessment of an applicant's criminal history before employers take any adverse action against an individual, such as rescinding a conditional job offer. The assessment must consider whether the applicant's criminal history has a "direct adverse and negative bearing" on their ability to perform the duties or responsibilities necessarily related to the applied-for position, such that it "justifies" denying employment. The employer's assessment must consider the factors outlined in the state law, such as the amount of time that has passed since the criminal conduct or completion of sentence.[4]

The ordinance requires a form of "pre-adverse" action notice before an employer takes adverse action against the individual based, in whole or in part, on their criminal history. The contents of the notice are mandatory and include informing the applicant of the right to submit evidence of rehabilitation.[5] Importantly, a copy of the documented, written individualized assessment must be enclosed with the notice. The notice must be sent by both mail and e-mail if the employer has the individual's e-mail address.

The employer may not take adverse action or fill the employment position for at least five business days after the candidate has received this notification. If the candidate provides the employer with certain information within this five-business-day period, such as that they are disputing the criminal history in the criminal background report, the employer must defer any final decision for at least 10 additional business days. Applicants must have the opportunity to arrange to meet with the employer to present this information verbally if they request such a meeting.

Employers must consider any additional information timely submitted by an applicant before making a final decision. This further assessment also must be documented in writing.

If an employer decides to take adverse action, a form of "adverse action" notice is required. The contents of the notice are mandatory, including enclosing a copy of the second individualized assessment and notifying the individual of the right to submit a complaint to DCBA for violations of the ordinance, and with the state's Civil Rights Department for violations of the state law. It must be sent by both mail and e-mail if the employer has the individual's e-mail address. Notices sent more than 30 days after an individual's response to the initial notice are deemed untimely and violate the ordinance. However, the employer can rebut this presumption with evidence justifying why it could not make the decision within 30 days.

Record Retention

The ordinance requires employers to retain pertinent records for a minimum of four years.

Enforcement and Exhaustion

The ordinance authorizes public and private remedies, including civil claims. An aggrieved individual may not file a private lawsuit against an employer unless and until they first meet certain exhaustion requirements.

Recommendations

Employers with operations in, or that do business or have contracts with, the County, at a minimum, 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. Suggested action items for employers with employees in the County and other jurisdictions having ban-the-box 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;
- Plan for the requirement to prepare additional documentation for the individualized assessment and record retention;
- Plan for delays in filling staffing openings due to delays in receiving background reports; 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.

Click Here for the Original Article

California's Privacy Laws: Financial and Medical Data, Website Usage, Children's Data, Data Brokers, and Customer Records

California has a long history of protecting privacy rights. Article I, Section 1, of the California Constitution expressly provides a right of privacy. Recently, the focus has been on compliance with the California Consumer Privacy Act (CCPA), which provides a complex set of compliance issues, particularly for companies that employ California residents.

Quick Hits

- California laws protect consumers' privacy rights regarding, among other things, financial and medical data, website usage, and telephone conversations. They also require businesses to eventually dispose of customer records containing personal information.
- Businesses are required to implement security procedures and practices with respect to personal information about California residents.
- Businesses with operations in California are required to disclose data breaches to California customers.

In addition to the CCPA, the California Constitution and state statutory law provide for a number of privacy rights and protections. More lawsuits have been popping up recently based on alleged privacy violations. Below is a summary of some key privacy laws that companies need to be aware of in order to navigate the California privacy landscape. This is not an exhaustive list; for example, there are numerous industry-specific privacy laws—such as those applicable to insurance companies, telecommunications companies, and state agencies—and there are other state law adoptions of federal law standards (such as background checks) that are not listed below.

California Constitutional Privacy Rights (Cal. Const., Art. I, § 1)

The California Constitution enshrines the right to privacy as an inalienable right of all individuals, and enforcement of privacy rights under the California Constitution is upheld through private right of action. To prevail in a privacy lawsuit, a plaintiff must demonstrate a legally protected privacy interest, a reasonable expectation of privacy in the circumstances, and conduct by the defendant constituting a serious invasion of privacy.

California Online Privacy Protection Act of 2003 (Cal. Bus. & Prof. Code §§ 22575–22579)

The California Online Privacy Protection Act (CalOPPA) addresses the privacy notice disclosure obligations of an operator of a commercial website or online service (collectively, "website") that gathers personally identifiable information from California residents, not limited to those based within the state. A website operator that collects personally identifiable information of California residents through the internet is required to "conspicuously post its privacy policy" on its website. The term "personally identifiable information" means "individually identifiable information about an individual consumer collected online by the operator" from that individual "and maintained by the operator in an accessible form." The website operator's privacy policy must outline what personally identifiable information is collected, with whom it may be shared, and how consumers can review and request changes to their information. Additionally, the policy must describe how the website responds to web browser "do not track" signals and whether third parties may collect personally identifiable information about an individual's online activities over time and across different websites.

Among other things, the California Legislature intended for this law to require each website operator to provide California resident consumers who use or visit the website with notice of its privacy policies, thus improving the knowledge these individuals have as to whether personally identifiable information obtained by the website may be disclosed, sold, or shared.

California Invasion of Privacy Act (Cal. Penal Code §§ 630–638.55)

The California Invasion of Privacy Act (CIPA) replaced laws that permitted the recording of telephone conversations with the consent of one party to a conversation. In 2002, in *Flanagan v. Flanagan*, the California Court of Appeal, Fourth District, clarified that the purpose of the law was to provide privacy protections "by, among other things, requiring that all parties consent to a recording of their conversation." Citing *Flanagan*, the same court stated in 2011 that CIPA prohibits recording or monitoring done without consent, "regardless of the content of the conversation or the purpose of the monitoring, and is intended to protect rights separate and distinct from the right to prevent the disclosure of improperly obtained private information."

Under CIPA, the following conduct is prohibited:

- "[I]ntentionally tap[ping], or mak[ing] any unauthorized connection … with any telegraph or telephone wire, line, cable, or instrument, including … any internal telephonic communication system." Through additional code sections, this has been updated to include all types of recording devices.
- "[W]illfully and without the consent of all parties to the communication, or in any unauthorized manner, read[ing], or attempt[ing] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit."
- "[U]s[ing], or attempt[ing] to use … or to communicate in any way, any information [collected in violation of this law], or aid[ing], agree[ing] with, employ[ing], or

conspir[ing] with any person or persons to unlawfully do, or permit, or cause to be done any of the acts" described in this law.

Violations of CIPA are punishable by a fine not exceeding $2,500 or by imprisonment in the county jail not exceeding one year. The statutory damages provision makes CIPA a desirable target for plaintiffs seeking recovery of damages without demonstrating any actual harm, subject to traditional principles of standing. As a result, CIPA litigation surrounding the use of online web tracking technology has been soaring in recent years. Ogletree Deakins will follow up soon with a more in-depth summary and update on CIPA litigation.

California Financial Information Privacy Act (Cal. Fin. Code §§ 4050–4060)

The purpose of the California Financial Information Privacy Act (CFIPA) is to require financial institutions to provide their consumers notice and meaningful choice about how their nonpublic personal information is shared or sold by their financial institutions. "Nonpublic personal information" means "personally identifiable financial information (1) provided by a consumer to a financial institution, (2) resulting from any transaction with the consumer or any service performed for the consumer, or (3) otherwise obtained by the financial institution."

Subject to some exceptions, CFIPA restricts financial institutions from disclosing nonpublic personal information to nonaffiliated third parties without the consumer's explicit prior consent. For sharing information with affiliates, CFIPA requires financial institutions to notify consumers annually in writing and allow them the option to opt out of such information sharing. Importantly, CFIPA outlines specific scenarios where consumer consent is not required for the disclosure of personal information, such as circumstances necessary for completing transactions requested by the consumer, maintaining or servicing accounts, complying with legal and regulatory requirements, preventing fraud, and several other specified activities. Financial institutions are also required to adopt measures ensuring the confidentiality of consumer information when engaging in these exempted disclosures. Moreover, financial institutions must adhere to strict consent procedures before sharing nonpublic personal information with nonaffiliated third parties. This includes obtaining written consent from consumers through a clear and conspicuous form that details the nature of the consent and informs consumers of their rights, including the ability to revoke consent at any time.

Confidentiality of Medical Information Act (Cal. Civil Code §§ 56–56.37)

The Confidentiality of Medical Information Act (CMIA) establishes strict guidelines to protect the confidentiality of individuals' medical information, and it supplements federal protections under the Health Insurance Portability and Accountability Act (HIPAA) by providing additional requirements for the handling of medical information by health care providers, health care service plans, pharmaceutical companies, and contractors in California. Under the CMIA, "medical information" is defined broadly to include "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor."

This encompasses a patient's medical history, mental or physical condition, or treatment details, along with any personal identifying information sufficient to allow identification of the individual. Unauthorized disclosure of medical information is prohibited unless explicit authorization is obtained, except in specified circumstances such as legal proceedings, administrative investigations, and efforts to diagnose or treat the patient, among other exceptions

Among other remedies, the CMIA provides for an award of $1,000 in nominal damages to a patient if the health care provider negligently releases medical information or records in violation of the act. Furthermore, entities that knowingly and willfully obtain, disclose, or use medical information in violation of the CMIA may be subject to an administrative fine of up to $2,500 per violation. No breach of confidentiality takes place until an unauthorized person views the medical information. It is the medical information, not the physical record (whether in electronic, paper, or other form), that is the focus of the act.

Customer Records (Cal. Civil Code §§ 1798.80–1798.84)

California's customer records law under Civil Code §§ 1798.80–1798.84 requires that a business "take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means." "Personal information" is defined as "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual."

Security Procedures and Practices

Businesses are required to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, [and] to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." The law provides a detailed discussion of what constitutes personal information, which includes an "individual's first name or first initial and last name" in combination with such things as a Social Security number, driver's license number, or California identification number, or medical information and account information, along with several other categories.

Disclosure Requirements After Breaches

The customer records statute also requires providing notification of data breaches to affected individuals, in addition to notifying the California attorney general, where notification is provided to more than 500 California residents. A "data breach" is defined as unauthorized acquisition of either (i) unencrypted personal information or (ii) encrypted personal information with the encryption key or security credential.

The statute furthermore requires notification "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement … or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." If the entity experiencing a breach does not own the data at issue (such as in the case of a service provider), it must notify the data owner or licensee "immediately." Importantly, the acquisition of personal information in good faith by an employee or agent of the entity for the entity's purposes does not constitute a breach, provided the "information is not used or subject to further unauthorized disclosure." The law also mandates very specific notice content requirements. If Social Security numbers or government identification numbers are compromised, businesses are required to provide affected individuals with an offer for free identity theft prevention and mitigation services for a period of at least twelve months.

Digital Privacy Rights for Minors (Cal. Bus. & Prof. Code §§ 22580–22582)

The Privacy Rights for California Minors in the Digital World Act, enacted in 2013, addresses the unique privacy challenges faced by children in the online environment. This law prohibits operators of websites, online services, applications, or mobile apps directed at minors from engaging in certain advertising practices, such as promoting tobacco, alcohol, or firearms to minors. The law defines a minor as any natural person under eighteen years of age residing in California and specifies what constitutes an online platform directed at minors. It also outlines the obligations of operators regarding the use and disclosure of minors' personal information, especially in the context of marketing and advertising.

Key provisions of the Privacy Rights for California Minors in the Digital World Act include:

- *Advertising restrictions*. Operators of online platforms catering to minors are prohibited from advertising certain products that may be harmful or inappropriate for children.
- *Protection of minors' online experiences*. The law aims to shield minors from exposure to potentially harmful content and influences while navigating the digital landscape.

While the Privacy Rights for California Minors in the Digital World Act lacks express enforcement provisions, violations may be addressed through California's Unfair Competition Law, underscoring the state's commitment to protecting children's online privacy.

Student Online Personal Information Protection Act (Cal. Bus. & Prof. Code § 22584–85)

Enacted in 2014, the Student Online Personal Information Protection Act (SOPIPA) aims to safeguard the privacy of K-12 students' personal information collected and maintained by online platforms used for educational purposes. Businesses providing services to K-12 students, including those involved in educational technology and services beyond California but serving California students, must comply with SOPIPA's requirements. The law prohibits operators of such websites or services from using students' personally identifiable information for targeted advertising or creating profiles for commercial purposes.

Key provisions of SOPIPA include:

- *Prohibition on targeted advertising*. SOPIPA prohibits the use of students' personal information for targeted advertising or creating user profiles for noneducational commercial purposes. This means operators cannot use the data collected from K-12 students to direct specific advertisements to them based on their online behavior or information gathered through educational services.
- *Restrictions on data sharing*. The law restricts how student data can be shared with third parties. Operators are barred from selling student information and are only allowed to disclose data under specific circumstances that further educational purposes, ensuring a higher degree of privacy for students.
- *Information protected*. SOPIPA safeguards "Covered Information," which includes a broad range of personally identifiable information provided by students or collected by operators through educational services. This encompasses educational records, biometric data, contact information, disciplinary records, test results, and more, ensuring comprehensive protection of students' data.
- *Security and deletion requirements*. Operators must implement reasonable security measures to protect students' information from unauthorized access and other threats. Additionally, they are required to delete covered information upon request from the school or district, providing a mechanism for the removal of student data from online platforms when no longer needed.

While SOPIPA does not have explicit enforcement provisions, violations may be enforced through California's Unfair Competition Law.

California Age-Appropriate Design Code Act (Cal. Civ. Code §§ 1798.99.28–1798.99.40)

California recently passed the California Age-Appropriate Design Code Act, marking a significant development in state law privacy protections for minors' data that is set to take effect on July 1, 2024. Under the act, any business providing online services likely to be accessed by children under eighteen years of age faces affirmative requirements and prohibitions on certain data practices. Inspired by the United Kingdom's Age-Appropriate Design Code, the act imposes burdensome obligations, including the completion of data protection impact assessments (DPIA), implementation of privacy protective default settings, and adherence to age-tailored transparency requirements. The broad language of the act presents challenges for designing compliance programs, with uncertainty surrounding potential regulatory guidance from the California attorney general.

Notably, in September 2023, the U.S. District Court for the Northern District of California entered a preliminary injunction in *NetChoice, LLC v. Bonta*, No. 22-cv-08861, blocking the law from taking effect. The California attorney general has appealed that decision, and the appeal remains pending before the Ninth Circuit Court of Appeals. Ogletree Deakins will continue to monitor that appeal for updates.

If the law is allowed to take effect following an appeal, key provisions of the act include age estimation measures, requiring businesses to assess whether their services, products, or features are "likely to be accessed by children," and to implement age-gating or data collection limits for age estimation purposes. DPIAs are mandated for new online services likely to be accessed by children, with businesses required to identify risks of material detriment to children and develop mitigation plans. Additionally, default privacy settings must offer a high level of privacy, and transparency requirements must be tailored to the age of the children accessing the service.

Enforcement of the act will be overseen by the California attorney general, with violators facing injunctions and civil penalties of up to $7,500 per affected child for intentional violations. While the act prohibits a private right of action, businesses may want to consider proactively addressing compliance to avoid regulatory scrutiny and potential penalties. The act's emphasis on protecting children's physical and mental well-being underscores the importance of responsible data practices in the online environment, setting a precedent for children's privacy protection nationwide and a likely model for other states to follow.

Data Broker Registration (Cal. Civ. Code §§ 1798.99.80–1798.99.89)

Effective January 1, 2020, the data broker registration law requires data brokers to register with the California attorney general and disclose pertinent information about their business practices. A "data broker," as defined by the law, refers to "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." In October 2023, Governor Gavin Newsom signed into law Senate Bill (S.B.) 362, the Delete Act, which overhauled the data broker law to include more detailed registration and reporting requirements, expansion of metrics related to consumer rights requests, and the creation of a new deletion mechanism for consumers that is required to be implemented by January 1, 2026. Beginning on that date, data brokers must process all pending deletion requests at least once every forty-five days, and direct their contractors and service providers to also delete such information, among other requirements. Following passage of the Delete Act, the California Privacy Protection Agency (CPPA) is now responsible for registrations rather than the California attorney general, and the CPPA will maintain a publicly accessible website to publish information provided by data brokers.

Failure to register as a data broker incurs penalties, including civil fines and injunctions. The penalties include $200 for each day that a broker fails to register with the CPPA, and an administrative fine of $200 per deletion request every day that a broker fails to delete personal information where required.

Click Here for the Original Article

City of Columbus Bans Consideration of Salary History in the Hiring Process

Beginning on March 1, 2024, the City of Columbus will ban consideration of salary and wage history during the hiring process for all employers in the City with fifteen or more employees. In so doing, Columbus joins a growing list of states and political subdivisions that, in an effort to promote pay equity, have enacted similar bans.

Inquiries into salary and wage history have become controversial in light of the evidence that women often earn less money than men for equal or similar work, and such inquiries have the effect of or potential to perpetuate such discrimination as well as continue to suppress women's wages.

The ban will apply with respect to "applicants," which term is defined as any person applying for employment to be performed in the City, and whose application will be considered in the City, regardless of whether the applicant is interviewed or not. Employers may not make inquiries as to salary or wage history (which includes benefits and other means of compensation) to the applicant or the applicant's previous employers for the purpose of obtaining the salary or wage history. Additionally, they may not conduct a search of publicly available records or reports to determine an applicant's salary or wage history.

So, what is permitted? An employer may still provide information on the proposed salary or wage range for the position being sought, and may continue to have discussions with an applicant about the applicant's salary requirements or expectations for the position sought.

Finally, the ordinance provides for a complaint procedure and civil penalties for employers found to have violated the ordinance's provisions.

What to do now? If your business is located in Columbus and you have fifteen or more employees, here are several actions you should take immediately to ensure compliance with the new ordinance.

- Examine your employment applications and job postings, whether paper or electronic, and remove any inquiry into past salary, wages, or benefits or any requirement to disclose such information.
- Educate your internal recruiters about the new ordinance and ensure that outside recruiters are aware of it and its requirements as well.
- Provide guidance and/or training to those in your company who conduct interviews with applicants as to the prohibitions on such inquiries and ensure that any interview guides or "scripts" are free from directives to make such inquiries.

Click Here for the Original Article

New Hampshire Passes Comprehensive Consumer Data Privacy Law

On March 6, 2024, New Hampshire's Governor signed Senate Bill 255, which establishes a consumer data privacy law for the state. The Granite State joins the myriad of state consumer data privacy laws. It is the second state in 2024 to pass a privacy law, following New Jersey. The law shall take effect **January 1, 2025.**

To whom does the law apply?

The law applies to persons who conduct business in the state or persons who produce products or services targeted to residents of the state that during a year period:

- Controlled or processed the personal data of not less than 35,000 unique consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or,
- Controlled or processed the personal data of not less than 10,000 unique consumers and derived more than 25 percent of their gross revenue from the sale of personal data.

The law excludes certain entities such as non-profit organizations, entities subject to the Gramm-Leach-Bliley Act, and covered entities and business associates under HIPAA.

Who is protected by the law?

The law protects consumers defined as a resident of New Hampshire. However, it does not include an individual acting in a commercial or employment context.

What data is protected by the law?

The law protects personal data defined as any information linked or reasonably linkable to an identified or identifiable individual. Personal data does not include de-identified data or publicly available information. Other exempt categories of data include without limitation personal data collected under the Family Educational Rights and Privacy Act (FERPA), protected health information under HIPAA, and several other categories of health information.

What are the rights of consumers?

Consumers have the right under the law to:

- Confirm whether or not a controller is processing the consumer's personal data and accessing such personal data
- Correct inaccuracies in the consumer's personal data
- Delete personal data provided by, or obtained about, the consumer
- Obtain a copy of the consumer's personal data processed by the controller

- Opt-out of the processing of the personal data for purposes of target advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects. Although subject to some exceptions, a "sale" of personal data under the New Hampshire law includes the exchange of personal data for monetary or other valuable consideration by the controller to a third party, language similar to the California Consumer Privacy Act (CCPA).

When consumers seek to exercise these rights, controllers shall respond without undue delay, but no later than 45 days after receipt of the request. The controller may extend the response period by 45 additional days when reasonably necessary. A controller must establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of the decision. As with the CCPA, controllers generally may authenticate a request to exercise these rights and are not required to comply with the request if they cannot authenticate, provided they notify the requesting party.

What obligations do controllers have?

Controllers have several obligations under the New Hampshire law. A significant obligation is the requirement to provide a "reasonably accessible, clear and meaningful privacy notice" that meets standards established by the secretary of state and that includes the following content:

- The categories of personal data processed by the controller;
- The purpose for processing personal data;
- How consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;
- The categories of personal data that the controller shares with third parties, if any;
- The categories of third parties, if any, with which the controller shares personal data; and
- An active electronic mail address or other online mechanism that the consumer may use to contact the controller.

This means that the controller needs to do some due diligence in advance of preparing the notice to understand the nature of the personal information it collects, processes, and maintains.

Controllers also must:

- Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. As with other state data privacy laws, this means that controllers must give some thought to what they are collecting and whether they need to collect it;
- Not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer unless the controller obtains the consumer's consent;

- Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue. What is interesting about this requirement, which exists in several other privacy laws, is that this security requirement applies beyond more sensitive personal information, such as social security numbers, financial account numbers, health information, etc.;
- Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with COPPA. Sensitive data means personal data that includes data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying an individual; personal data collected from a known child; or, precise geolocation data;
- Not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers;
- Provide an effective mechanism for a consumer to revoke the consumer's consent that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request; and
- Not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge, and willfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age.
- Not discriminate against a consumer for exercising any of the consumer rights contained in the New Hampshire law, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

In some cases, such as when a controller processes sensitive personal information as discussed above or for purposes of profiling, it must conduct and document a data protection assessment for those activities. Such assessments are required for the processing of data that presents a heightened risk of harm to a consumer.

Are controllers required to have agreements with processors?

As with the CCPA and other comprehensive data privacy laws, the law appears to require that a contract between a controller and a processor govern the processor's data processing procedures with respect to processing performed on behalf of the controller.

Among other things, the contract must require that the processor:

- Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
- At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law.
- Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;
- After providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and
- Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under the law, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

Other provisions might be appropriate in an agreement between a controller and a processor, such as terms addressing responsibility in the event of a data breach and specific record retention obligations.

How is the law enforced?

The attorney general shall have sole and exclusive authority to enforce a violation of the statute.

Click Here for the Original Article

New Washington, D.C. Pay Transparency Law Scheduled to Go Into Effect on June 30, 2024

Washington, D.C. joins a growing group of states requiring employers to include projected salary ranges in job postings and to restrict the use of pay history in setting pay.

On Jan. 12, 2024, the mayor of D.C. signed the Wage Transparency Omnibus Amendment Act, which, among other things, requires private employers, regardless of size, to disclose pay ranges in all job postings and advertisements. Because the D.C. budget is controlled by Congress, the Amendment was sent to Congress for a 30-day review on Jan. 22, 2024, with a projected law date of March 9, 2024. The new law is scheduled to go into effect on June 30, 2024.

The Amendment requires employers to include in job postings the minimum and maximum projected salary or hourly wage for the position. Employers not only must disclose the projected salary in public job postings, but they also must do so in any internal job postings of the position. The Amendment also requires employers to disclose to prospective employees the existence of other benefits (such as healthcare or bonuses) before the first interview.

The Amendment prohibits employers from screening job applicants based on wage history. The Amendment does not specifically address remote positions.

Employers will be required to post a notice in the workplace notifying employees of their rights under this law. The notice must be posted in a conspicuous place in at least one location where employees congregate.

The new requirements under the Amendment will also affect the PERM labor certification process for employers sponsoring foreign nationals for "green cards." Employers can prepare for these changes by:

- Reviewing and modifying, as needed, all recruitment postings (both external and internal) to ensure these postings include the required salary ranges.
- Reviewing internal interviewing protocols to ensure disclosure of benefit information upon request or before conducting a screening interview (whether by phone or in person) with an applicant for the PERM position.
- Reviewing internal interviewing protocols to ensure no historical pay information is requested from prospective employees or from their prior employers. Indeed, this would not even be relevant because the applicant for the PERM position will know the salary range.
- Training employees involved in the PERM process on the benefit disclosure requirements and the salary history restrictions.

The law aims to increase pay equity and to address historical wage gaps. While the law does not create a private right of action for employees, the Amendment provides the attorney general the authority to investigate violations and to bring civil actions against an employer or seek remedies on behalf of individuals or the public. Employers found to have violated the law may be subject to civil fines ranging from $1,000 to $20,000 per occurrence.

Click Here for the Original Article

New York City Employers Must Provide Workers' Bill of Rights by July 1

On Jan. 3, 2024, New York City's Local Law 161 took effect, authorizing the City to publish a "workers' bill of rights." New York City employers must comply with the law's notice and posting requirements by July 1, 2024.

The law required the Department of Consumer and Worker Protection, in coordination with the City's agencies on immigration and human rights as well as community and labor organizations, to publish a workers' bill of rights by March 1, 2024. The workers' bill of rights, which is now live on the City's website here, contains information on workers' rights and protections under federal, state, and local laws that apply to all workers in New York City, regardless of immigration status.

Beginning July 1, 2024, New York City employers must provide copies of the workers' bill of rights to all employees, and to new employees upon hire. Employers must also post the workers' bill of rights in in the workplace and on the company's intranet and mobile application, if applicable. Employers must post and distribute this notice in English as well as any language spoken as a primary language by at least five percent of the employer's workforce, if the notice is available in that language. Currently, the workers' bill of rights is available for translation in 133 languages.

First violations of Local Law 161 will be granted a 30-day grace period to cure, and subsequent violations are subject to a $500 civil penalty. The law does not specify what constitutes a "violation."

Takeaways

New York City employers should take steps to comply with the notice and posting requirements of Local Law 161 by the July 1, 2024 deadline. Employers should also review the workers' bill of rights to ensure ongoing compliance with all legal obligations and protections listed on the notice.

Click Here for the Original Article

Virginia governor vetoes "salary history ban" statute legislation

On March 14, 2024, Virginia Governor Glenn Youngkin (R) vetoed identical bills passed by the Virginia legislature barring employers from asking about a job applicant's salary history and requiring pay information to be included in job listings.

Senate Bill 370 and House Bill 990, introduced by Senator Jennifer Boysko (D) and Delegate Michelle Maldonado (D), respectively, add a new "salary history ban" statute to the Chapter of the Virginia Code that provides protections for employees. The legislation passed along party lines, with support from Democratic majorities in both the House and the Senate.

The proposed legislation prohibits prospective employers from (i) asking job applicants for their wage or salary history; (ii) relying on that history in determining the applicant's starting wage or salary; (iii) considering wage or salary history when making a hiring determination; and (iv) refusing to interview, hire, employ, promote, or otherwise retaliate against an applicant for not providing wage or salary history. It also requires prospective employers to disclose the wage, salary, or wage or salary range for public and internal job postings. The legislation also creates a cause of action for aggrieved applicants and employees and provides for statutory damages between $1,000 and $10,000 or actual damages, whichever is greater, reasonable attorney's fees and costs, and other appropriate relief.

In a formal explanation of his veto, Governor Youngkin acknowledged the importance of addressing wage disparities, but said that the legislation "represents government overreach, offering incomplete information during the hiring process, disregarding business needs, and potentially exposing small businesses to lawsuits." He described the legislation as a "one-size-fits-all approach" that disregards the diverse nature of Virginia businesses and that its "potential adverse effects on small businesses, prospective employees, and the economy are too high."

An increasing number of states have adopted "salary history ban" statutes or other similar policies. According to the National Conference of State Legislatures (NCSL), several states, including California, Colorado, Illinois, New York, and Washington, mandate the inclusion of salary ranges in job postings. Connecticut, Maryland, Nevada, and Rhode Island require employers to disclose salary ranges by default or upon request during the interview process, though not in job postings. Some states, including Alabama, Delaware, Hawaii, and Minnesota, ban employers from asking applicants for their salary history.

The Virginia General Assembly will reconvene on April 17, 2024, to consider the Governor's proposed recommendations to and vetoes of bills. A 2/3 vote of each body is required to override a Governor's veto. While Democrats hold majorities in both chambers, neither majority is large enough to overcome a veto without bipartisan support.

Click Here for the Original Article

Housing Authority to issue guidance on background checks

Blaine County Housing Authority staff members will start a new effort to inform agency landlords about guidelines for conducting criminal background checks, following a decision from the agency's board during its Wednesday, March 13, meeting.

"We're recommending that each time we send [landlords] an applicant lead, we provide a letter reminding them [of rules] as well as requiring annual landlord certification of compliance with fair housing [rules]," Ketchum Housing Director Carissa Connelly said during the meeting.

BCHA does not currently receive confirmation from landlords that they are conducting background checks on BCHA-referred housing applicants in a manner that complies with federal fair housing rules, according to a memo describing why the board was asked to approve the action. And prospective tenants with criminal records are having trouble finding housing even when the incidents that created a criminal record happened long ago or weren't related to housing stability.

The U.S. Department of Housing and Urban Development allows a permanent ban on a candidate for housing in two cases: if the household includes someone required to register as a sex-offender for life, or if the household includes someone who has been convicted of manufacturing methamphetamine on a federally-assisted property.

HUD also permits a ban on housing admission for three years if a household member has been evicted from federally-assisted housing for drug-related criminal activity. However, housing authorities have discretion in this case if the member has successfully completed rehabilitation or if the circumstances leading to the eviction no longer exist—for example, if the member of the household who committed the crime is incarcerated or deceased.

The BCHA wants to ensure that these rules, among others, are uniformly applied. The letter the agency will send to landlords notes that applicants may not be denied housing based on arrest records and that blanket bans on criminal history may not be applied. Additionally, the drafted letter states that background checks must be conducted consistently. Connelly explained the process for verifying an applicant's status further.

"For [crimes other than lifetime sex offenses] we recommend [meeting] with probation officers, [and] conducting a background check for evictions," she said. "Determining if a reason for conviction is a potential risk to the health and safety of residents in the building and also determining if the applicant is on probation. If they are in good standing, we would let them move in. If they are not, they would be denied."

BCHA board members unanimously approved the new landlord outreach.

Click Here for the Original Article

Massachusetts Latest State Expected to Restrict Access to Credit Reports for Employment Purposes

On March 14, 2024, the Massachusetts House of Representatives passed legislation that would add a new provision to the Massachusetts Consumer Protection law and would bar the use of true credit reports for employment purposes, *i.e.*, for the purpose of evaluating an individual for employment, promotion, reassignment, or retention as an employee. The legislation, entitled *An Act Reducing Barriers to Employment Through Credit Discrimination* (H.1434), is expected to be adopted by the Massachusetts Senate and promptly signed into law by Governor Maura Healy. Once adopted, the new law would take effect on January 1, 2025, and would be the most restrictive of its kind in the United States.[1]

The law would bar an employer from requesting from a consumer reporting agency (background check company or credit bureau) a consumer report that bears on an individual's "credit worthiness, credit standing or credit capacity." The law would prohibit the use of any such information as a factor in establishing an individual's eligibility for employment, promotion, reassignment, or retention. Further, the law would forbid an employer from requiring an individual to answer questions about the contents of a consumer report or the information contained in it regarding credit worthiness, credit standing or credit capacity. Note that the new law would apply only to true credit reports and would not affect employers' ability to obtain other background checks (*e.g.*, criminal record checks, driving record checks, education or employment verifications, etc.).[2]

Violations of the new statute would constitute unfair trade practices under the Massachusetts Consumer Protection law, Chapter 93A, which allows for awards of attorneys' fees, costs, and, when a violation is willful or knowing, double damages.

In contrast with credit reporting laws in other states, some of which broadly allow credit checks for jobs involving proprietary or confidential information (*e.g.*, California), the bill passed by the Massachusetts House contains very narrow exemptions. The only exemptions are for employers (such as registered securities associations) required by federal or state law to conduct credit checks, for employees or applicants who hold positions requiring a national security clearance, and for employees working at financial institutions.

The bill contains an anti-retaliation and anti-discrimination provision that prohibits employers from taking adverse action against an individual because they have or intend to:

- file a complaint alleging a violation of Chapter 93A or the new law;
- participate, assist, give evidence, or testify in a proceeding or an action concerning a violation of the new law; or
- oppose a violation of the new law.

Finally, waivers of the law would be void and employers could not require or request that employees or applicants waive their rights under the law.

Action Steps for Employers

If the bill is enacted, before January 1, 2025, employers operating in Massachusetts that use consumer credit reports for employment purposes should assess whether they can continue to do so. Most private sector employers will no longer have access to such reports.

Employers should evaluate the contents of the documents they use in conjunction with their screening procedures and modify the paperwork as needed to reference the new law. While there is no additional notice provision in the language of the bill, employers may want to proactively notify employees and applicants that no consumer reports concerning their credit worthiness, credit standing, or credit capacity will be requested or used for employment purposes.

Click Here for the Original Article

Hawaii Senate Passes Recreational Marijuana Legalization Bill

The Hawaii state Senate on Tuesday passed a bill to legalize recreational marijuana for adults and create a regulated and taxed market for adult-use cannabis. After approval in the Senate by a vote of 19-6, the legislation now heads to the state House of Representatives, where cannabis reform advocates hope new amendments will be made to the measure.

If passed by the House and signed into law by the governor, the legislation (Senate Bill 3335) would allow adults aged 21 and older to possess up to one ounce of marijuana and up to five grams of cannabis concentrates. The measure, which would go into effect on January 1, 2026, would also permit the home cultivation of up to six marijuana plants and allow for the possession of up to two pounds of harvested homegrown weed. The bill was introduced in the legislature in January and was approved by Senate legislative committees in February and earlier this week.

The bill, which is largely based on a weed legalization proposal released by Hawaii Attorney General Anne Lopez last year, would also create a new state agency to regulate hemp, medical marijuana and adult-use cannabis. Dubbed the Hawaii Hemp and Cannabis Authority, the agency would be tasked with licensing cannabis and hemp businesses and regulating the industry. The legislation would also create a five-member Cannabis Control Board for oversight of the new agency.

The cannabis legalization bill also expunges the records of past arrests and convictions for actions that are permitted or decriminalized under the measure, including marijuana possession charges. Petition-based expungements would begin on January 1, 2026, including petitions to review cannabis-related sentences.

Cannabis Activists Seek Changes To Bill

While acknowledging the progress made with the passage of the marijuana legalization bill in the Hawaii Senate, many cannabis policy advocates are critical of provisions of the measure that create new criminal penalties for some actions. The Hawai'i Alliance for Cannabis Reform (HACR) notes in a brief that the bill creates an unscientific DUI law that sets an arbitrary limit of 10 nanograms per milliliter of THC in a driver's system, an amount that can remain long after impairment wears off. Another provision highlighted by reform advocates would subject those found with loose cannabis, a cannabis package that has ever been opened, or a marijuana pipe in an automobile to up to 30 days in jail.

Karen O'Keefe, director of state policies for the Marijuana Policy Project, said "Hawai'i is behind the times on cannabis policy reform, but 2024 could be the year that finally changes."

"Right now, Hawai'i lawmakers have the opportunity to not only pass legalization and regulation, but also to work to improve the bill to ensure it is rooted in justice and equity, not an excessively punitive approach," O'Keefe said in a statement from the marijuana policy reform advocacy. "Cannabis legalization is an essential criminal justice reform, and Hawai'i lawmakers should treat it as such by focusing far more on education, reinvesting in communities, reparative justice, and building an equitable and inclusive industry."

Activists with HACR have submitted proposals to amend SB 3335 to address what they see as shortcomings of the legislation. One proposed amendment would eliminate the *per se* THC limit for drivers, while another would eliminate the open container provisions of the bill. Additional proposed amendments from the group include clarifying that expungements and resentencing will be initiated by the state, removing restrictions on public consumption and the addition of provisions for small business and social equity licenses in the regulated cannabis market.

Nikos Leverenz of the Drug Policy Forum of Hawai'i and the Hawai'i Health and Harm Reduction Center called for the proposed amendments to be added to the legislation in the House of Representatives.

"Although this is an imperfect bill that still contains far too many elements of criminalization, it's welcome news to have a viable adult-use legalization bill that can be improved upon when it reaches the House," Leverenz said in an emailed statement. "Drug Policy Forum of Hawaii and other members of the Hawaii Alliance for Cannabis Reform are hopeful that our proposed amendments will be considered by the House Judiciary and Hawaiian Affairs Committee."

Legalizing recreational marijuana is supported by a majority of Hawaiians. A recent Hawai'i Perspectives poll found that 58% of the state's residents are in favor of "legalizing marijuana to allow possession, manufacture, and sale of marijuana by and to adults, under state licensing, regulation, and taxation."

If the bill is passed by the legislature and signed into law by Democratic Gov. Josh Green, Hawaii would join the other 24 states that have legalized recreational marijuana for adults.

Click Here for the Original Article

Florida Legislation Will Increase Background Screening for Healthcare Professionals

House Bill 975, if signed by Gov. Ron DeSantis, will have a significant impact on the Florida criminal background screening requirements for healthcare professionals and facilities. Currently, only certain healthcare professionals are required to undergo background screening as a requirement for licensure. Such professionals include the following: allopathic and osteopathic physicians, interns and fellows, physician assistants, chiropractic physicians and assistants, orthotists and prosthetists, podiatric physicians and podiatric x-ray assistants, certified nursing assistants, licensed practical nurses, registered nurses, advanced practice registered nurses, athletic trainers and massage therapists. However, the majority of healthcare professionals licensed by the Florida Department of Health are not required to undergo background screening as part of their initial licensure requirements.

If the bill becomes law, additional healthcare professionals licensed by the Department of Health will be required to undergo background screening as a requirement for initial licensure. The bill will also require certain individuals who are seeking licensure by endorsement to undergo background screening. Specifically, the following additional professionals will be required to undergo background screening:

- naturopaths
- optometrists
- pharmacists
- dentists and dental hygienists
- midwives
- occupational therapists
- opticians
- physical therapists
- speech-language pathologists
- nursing home administrators
- respiratory therapists
- dieticians
- electrologists
- clinical laboratory personnel
- medical physicists
- genetic counselors
- hearing aid specialists
- psychologists
- clinical social workers
- marriage and family therapists

- mental health counselors
- psychotherapists

Upon becoming law, such healthcare professionals licensed prior to July 1, 2024, will be required to complete the background screening requirements by July 1, 2025.

Potential Impact

This legislation will likely have a significant impact on healthcare professionals and facilities. For instance, if a healthcare professional has a disqualifying offense on his or her criminal record, the individual would be ineligible for employment. The individual would need to obtain an exemption from the appropriate state agency to be employed in a profession or workplace where background screening is statutorily required. Circumstances under which the head of an agency may grant an exemption from disqualification are very limited, and persons who are considered a sexual predator, career offender or registered sexual offender are ineligible for exemption.

Licensed healthcare facilities will need to update their background screening policies to ensure that these professionals undergo background screening. Such screening records, including the applicable employee roster, must be maintained and updated as necessary. Failure to comply with the statutory background screening requirements is one of the violations facilities are routinely cited for during a licensure survey.

Click Here for the Original Article

COURT CASES

Medical Marijuana Usage Is Not Protected Under the ADA, Vermont Federal Court Rules

On February 14, 2024, a judge of the U.S. District Court for the District of Vermont dismissed a plaintiff's Americans with Disabilities Act (ADA) discrimination and failure-to-accommodate case, holding that his medical marijuana usage was not protected under the ADA (*Skoric v. Marble Valley Regional Transit District*).

Quick Hits

- A federal district judge in Vermont ruled that the ADA does not protect medical marijuana usage.
- Under the federal Controlled Substances Act, marijuana has "no currently accepted medical use" and therefore does not fall under the supervised use exception of the ADA.

Marble Valley Regional Transit District terminated Ivo Skoric's employment after he failed a random drug test. According to his lawsuit, Skoric has a medical marijuana prescription to treat chronic pain and depression. Following his dismissal, Skoric sought unemployment benefits from the Vermont Department of Labor, which were denied.

Skoric filed his lawsuit *pro se*, alleging claims under the ADA for discrimination and failure to accommodate against Marble Valley, as well as seeking the denied unemployment benefits from the Vermont DOL. The unemployment claim was dismissed by the court for lack of subject matter jurisdiction.

In regards to the ADA claims, Marble Valley argued in its motion to dismiss that Skoric could not state a claim for either disability discrimination or failure to accommodate because he alleged that he was discharged for testing positive for marijuana on a random drug test, not because of his underlying disabilities. Marble Valley also argued that Skoric was not a qualified individual with a disability under the ADA because marijuana is an illegal drug under the federal Controlled Substances Act.

The ADA establishes that "a qualified individual with a disability shall not include any employee … who is currently engaging in the illegal use of drugs, when the covered entity acts on the basis of such use." Marble Valley argued that Skoric's marijuana usage falls under this provision, because it is a Schedule I illegal substance under the Controlled Substances Act. Skoric, on the other hand, relied on a different provision of the ADA, which allows for use of illegal drugs "taken under supervision by a licensed health care professional." Because he has a medical marijuana card, Skoric argued that he was using marijuana under the supervision of a doctor and thus protected by the ADA.

The court did not agree. In reaching its holding, the court cited other district court opinions, as well as a Ninth Circuit Court of Appeals decision, which concluded that medical marijuana use does not fall within the supervised-use exception of the ADA, and therefore outside the protections of the ADA. Citing *United States v. Oakland Cannabis Buyers' Co-op*, the court further reasoned that because marijuana has "no currently accepted medical use" under the Controlled Substances Act, a medical marijuana patient is not a "'qualified individual with a disability'" under the supervised-use exception of the ADA.

Next Steps

The opinion may seem like a knockout punch for employers doing business in Vermont that want to drug test their employees and take adverse action as a result of a negative drug test. However, employers may want to note that Vermont Statute Title 21, Chapter 5, Section 513, flatly prohibits random drug testing. The statute also requires that employers put employees through an employee assistance program (or comparable rehabilitation program) prior to termination of employment.

Employers may also want to note that this was a federal ADA case and, in turn, the "federally illegal" status of marijuana was likely a more pertinent consideration for the district court. State courts, especially in states like Vermont that have employee-friendly marijuana laws, may come out the other way when interpreting their own state anti–disability discrimination laws. In addition, numerous state courts across the country have recognized disability claims under state disability laws, and, at least in a smaller handful of states, the federal ADA. However, disability claims are always very fact-specific in nature.

Click Here for the Original Article

Connecticut Employers Can Terminate Employees Impaired by Medical Marijuana While Working; Appellate Court Also Provides Guidance for Reasonable Suspicion Drug Tests

In a significant decision about workplace drug use, the Connecticut Appellate Court backed an employer's right to terminate a worker who was impaired on the job by medical marijuana. The decision also clarified the factual basis an employer must possess to justify ordering a drug test based on suspicion of impairment.

In *Bartolotta v. Human Resources of New Britain, Inc.*, AC 46091 (Conn. App. Ct. Mar. 19, 2024), the court upheld the grant of summary judgment to an employer that was sued for allegedly violating Connecticut's Palliative Use of Marijuana Act (PUMA) and Urinalysis Drug Testing Statute. The decision marks the first time the Appellate Court has reviewed the merits of a private lawsuit under PUMA since such a cause of action was recognized by the Connecticut District Court in *Noffsinger v. SSC Niantic Operating Company, LLC*, 338 F. Supp. 3d 78 (2018). The Appellate Court's decision provides helpful guidance about what circumstances can justify reasonable suspicion drug testing under Connecticut law.

In the *Bartolotta* case, the defendant employed the plaintiff as a teaching assistant. When hired, the plaintiff held a prescribed medical marijuana card. The employer maintained written policies that explicitly prohibited employees from working while under the influence of any drug or alcohol.[1] The plaintiff did not disclose her use of medical marijuana.

On January 2, 2019, a teacher witnessed the plaintiff call a child by the wrong name. Confronted, the plaintiff said she was "just out of it," told the teacher she uses medical marijuana and acknowledged she was currently under its influence, saying "her head is just not right from it yet." Concerned for the welfare of the children, the teacher reported these facts to her supervisor. The defendant initiated an investigation, during which the plaintiff disclosed for the first time that she used medical marijuana to treat an underlying medical condition. She acknowledged that she had reported to work despite ingesting too much medical marijuana. The defendant suspended the plaintiff without pay and directed her to submit to a drug test, which came back negative for marijuana. Notably, a week had elapsed between the date of the incident and the date of the test.

Based upon the investigation, the defendant terminated the plaintiff's employment because she had admittedly been under the influence of marijuana at work, violating the terms of the drug and alcohol policy in the employee handbook.

The plaintiff sued the defendant alleging, among other things, violation of the PUMA and violation of the drug-testing restrictions of Connecticut General Statutes § 31-51x. The defendant sought and the trial court granted summary judgment, finding that the plaintiff failed to produce any evidence that the defendant had terminated her solely for being prescribed medical marijuana and that the defendant in fact did have reasonable suspicion to justify a drug test under the statute. On appeal the Appellate Court affirmed the trial court's grant of summary judgment.

Reaffirming Employer's Rights Under PUMA

The Appellate Court's decision clearly supports an employer's right to prohibit the use of marijuana in the workplace, even if the individuals affected have been certified to use medical marijuana under state law. The court emphasized the narrowness of claims that employees can make under PUMA: to prevail, a plaintiff must show that the employer terminated them solely because the employee had a prescription for medical marijuana.

In this instance, the plaintiff could not establish termination solely based on her status as a medical marijuana patient under PUMA since the investigation showed the plaintiff had admitted to being under the influence while at work and acknowledged that her conduct placed children under her care at risk. The court also noted that the employer had already suspended the plaintiff for this behavior before it was made aware of her status as a medical marijuana user. The decision may therefore serve as a helpful touchpoint on proactive steps employers are permitted to take to maintain a safe workplace even in jurisdictions where medical marijuana use is permitted by state law.

Reasonable Suspicion Standard for Testing

The Appellate Court's decision also provides helpful guidance about the meaning of the "reasonable suspicion" requirement of Connecticut's statutory limits on the circumstances under which employers can require urinalysis testing for drugs.

Connecticut General Statutes § 31-51x permits employers to require drug tests only if there is a reasonable suspicion of impairment affecting job performance. As the term "reasonable suspicion" is not specifically defined in the statute or associated regulations, the court in *Bartolotta* took the opportunity to review existing precedent and helpfully outline the appropriate standard.

Following the suggestion in a 1998 Connecticut Supreme Court case that the reasonable suspicion standard should align with the reasonable suspicion requirements of Fourth Amendment jurisprudence, the Appellate Court described the reasonable suspicion standard for drug testing as akin to that applied by police officers for searches and seizures. To have reasonable suspicion, the court said, requires that the employer have specific, articulable facts that would lead an objective reasonable person having such information to reach the same level of suspicion.

In the case at hand, the Appellate Court found that the investigation provided an adequate foundation for the defendant reasonably to conclude that the plaintiff had been impaired on the job, even though the drug test was requested approximately a week after the reported incident. The court said objective evidence confirmed the following: (1) the plaintiff had been observed by at least two witnesses acting "forgetful, droopy, and unsteady on her feet" during several weeks prior to the January 2, 2019 incident; (2) the plaintiff specifically admitted medical marijuana use to a colleague on that date and during the resulting investigation; (3) the plaintiff specifically admitted to using medical marijuana on a nightly basis and said she had consumed "too much" the night before the incident; (4) the plaintiff acknowledged that she had "messed up." Together, these pieces of evidence provided the employer with the level of reasonable suspicion necessary under the statute to justify its requirement that the plaintiff submit to a drug test.

The court's analysis underscores the challenge that employers face day-to-day when seeking to enforce reasonable drug testing policies in the workplace. The decision to mandate a reasonable suspicion drug test will necessarily be fact-specific and require employers to assess numerous sources of evidence to make the appropriate decision.

In light of this new guidance, employers that utilize reasonable suspicion drug testing are encouraged to review and assess current practices to ensure that the individuals responsible for making the assessment have a clear understanding of the objective standards to be applied and the importance of properly documenting the basis for the decision.

Click Here for the Original Article

INTERNATIONAL DEVELOPMENTS

EU Data Act: New Rules on Data Sharing And Portability of Cloud Services Now In Force

The EU Data Act came into force on January 11, 2024. The Data Act is part of the European Commission's data strategy released in February 2020 and obliges manufacturers of connected products to make use-related data available in certain circumstances. It also requires providers of data processing services (such as cloud services) to facilitate customers switching to a different provider, for instance, by providing minimal transitional services. Most of the new rules will apply as of September 12, 2025.

Connected products and extraterritoriality

Under the Data Act, connected products comprise products that obtain, generate or collect data concerning their use or environment, and that are able to communicate this data via electronic communications, physical connection or on-device access (such as IoT devices, e.g., connected home devices, medical devices or vehicles).

Obligations under the Data Act will mostly fall upon **manufacturers of connected products placed on the EU market** and providers of related services, **irrespective of their place of establishment**. Such companies – except micro, small or medium-sized enterprises – will be required to make use-generated data accessible to the user and to third-parties of the user's choice.

Key Impacts for In-Scope Businesses

The Data Act will impact manufacturers of connected products and providers of data processing services (including cloud services) with the key obligations below:

Obligations for Manufacturers of Connected Products Placed on the EU Market

- **Design**the product or service in a way that the use-generated data is easily accessible to the user;
- **Provide information**to the user about the data to be generated by the use of the product or service and how this may be accessed, retrieved or erased, **prior** to entering the contract with them;
- Upon request of the user, provide the use-generated data to the user or to a **third-party**, if the data is not directly accessible from the product or related service;
- Provide the data to the third-party chosen by the user under **fair, reasonable, transparent and non-discriminatory terms**, to be formalized in a contract. The Data Act **prohibits businesses from unilaterally imposing on other business "unfair" contractual terms**concerning access and use of data[1]span>. Such provisions also apply when a company is required to make data available to another company under EU or Member State law.
- Manufacturers or providers of related services may, on a case-by-case basis, **refuse**the sharing of specific data identified as **trade secrets**.[2] The refusal to share data may occur only in **exceptional circumstances**, where they are highly likely to suffer serious economic damage from the disclosure despite the technical and organisational measures taken by the user. The refusal must be based on **objective elements** (including the nature and level of confidentiality of the data at hand), duly substantiated and provided in writing to the user, and also notified to the national competent authority.

- Manufacturers or providers of related services may apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorised access to the data. However, smart contracts used to automate data-sharing are subject to certain requirements such as safe termination and interruption.
- Users and third-parties are **forbidden**from using the data to develop products that **compete** with the product from which the data is generated and from using the use-generated data to derive **insights** about the economic situation, assets and production methods of the manufacturer. Third-parties are only allowed to use the data for the purposes and under the conditions agreed with the user.
- Legal persons may be required to share data they hold with public sector bodies in **exceptional circumstances**, such as public emergencies, where the data could not be otherwise obtained by the public sector body in a timely and effective manner.

Obligations for Providers of Data Processing Services, Including Cloud Services

- **Facilitate customers switching**to other providers of the same service type, which includes refraining from imposing commercial, technical, contractual or organisational obstacles to a change of provider. In practice, this means that cloud providers will be required to provide certain minimum transitional services to customers which will be subject to limitations on charges which the providers can charge for their assistance. Such obligations will not apply where the main features of the service have been built to accommodate specific needs of an individual customer. These obligations have extraterritorial applications and apply to providers of data processing services, irrespective of their place of establishment, who provide service to customers in the EU.
- Take adequate technical, legal and organisational measures to **prevent international and third-country governmental access and transfer of non-personal data**held in the EU, if such transfer or access is illegal under EU or Member State law.

Fines

Member States shall lay down rules on penalties applicable to infringements of the Data Act. Fines to be imposed for infringements of data-sharing obligations may reach the amount of **EUR 20 million or 4%** of the total worldwide turnover of an entity for the preceding financial year, whichever is higher.

Next Steps

Most obligations under the Data Act will apply as of September 12, 2025. Obligations relating to the design and manufacturing of connected products will apply to the products and connected services placed on the market after September 12, 2026.

What Businesses Should Be Doing Now

Manufacturers of connected products and providers of related services are advised to **critically assess** their practices around providing data to users in view of the requirements of the Data Act and prepare a **roadmap** for implementation of compliance measures.

Providers of data processing services are likewise advised to consider the need for any changes to their practices (including technical and contractual measures) around switching and transitional assistance, interoperability and governmental access and transfer of non-personal data.

Privacy rules such as the GDPR, as well as cybersecurity regulations such as sectoral rules applying to medical devices and connected vehicles, may already apply in relation to products and services within the scope of the Data Act. In addition, new cyber rules are likely to be adopted soon with regard to connected devices – see our Legal Update on the draft EU Cyber Resilience Act from October 2023.

Furthermore, it is unclear how the Data Act will interact with other recently adopted pieces of legislation, such as the Digital Markets Act ("DMA"). In particular, the DMA has its own provisions on data portability in the DMA, and the Data Act prevents "gatekeepers" designated under the DMA from receiving user data. This illustrates how competition law and data-related rules are increasingly interconnected in the EU and often require a combined legal assessment.

These existing and forthcoming provisions should be taken into account when developing a compliance strategy.

[1] A contractual term is unfair if it "grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing". The Data Act lists terms which are always considered unfair (e.g., those excluding or limiting liability for intentional acts or gross negligence) and those that are presumed to be unfair.

[2] The Data Act relies on the definition of trade secrets in the Trade Secrets Directive (EU) 2016/943, which means that any business relying on the trade secrets exception must show that the information in question is subject to appropriate safeguards, among other things.

Click Here for the Original Article

Germany: Those 18+ May Legally Begin Possessing Cannabis Next Week

Legislation permitting the personal possession and home cultivation of limited amounts of cannabis cleared its final parliamentary hurdle on Friday.

Members of Parliament's upper house gave their approval to the measure. That vote followed approval from the lower chamber in February.

The measure allows residents ages 18 and older to possess (up to 25 grams) and home cultivate cannabis (up to three plants) beginning on April 1st. Not-for-profit cannabis clubs will be permitted to grow and provide cannabis for their members beginning on July 1st.

Neither commercial cannabis production, retail sales, nor marijuana-related advertising is permitted under the measure. Marijuana sales to minors will also remain strictly prohibited, with offenders facing penalties of up to two years imprisonment.

Last year, similar legislation took effect in the European nation of Luxembourg. That followed a similar move in 2021 by lawmakers on the island of Malta.

German lawmakers previously approved the limited use of medical cannabis products in 2017.

Click Here for the Original Article

MISCELLANEOUS DEVELOPMENTS

EU AI Act – Landmark Law on Artificial Intelligence Approved by the European Parliament

Summary

The highly anticipated EU Artificial Intelligence Act is finally here! With extra-territorial reach and wide-reaching ramifications for providers, deployers, and users of Artificial Intelligence ("*AI*"), the Artificial Intelligence Act ("*AI Act*") was finally approved by the European Parliament ("*EP*") on March 13, 2024. The text of the approved version is based on the political agreement that the EP reached with the Council of the European Union in December 2023. Members of the EP passed the law with 523 votes in favor, 46 against, and 49 abstentions. The Act aims to safeguard the use of AI systems within the EU as well as prohibiting certain AI outright.

The AI Act applies to:

- providers placing AI systems or models on the market in the EU or putting into service AI systems or placing on the market general-purpose AI models in the EU, irrespective of whether those providers are located within or outside the EU;
- deployers of AI systems that have their place of establishment in or who are located within the EU;
- providers and deployers of AI systems that have their place of establishment or who are located in a third country in situations where the output produced by the AI system is used in the EU;
- importers and distributors of AI systems into or within the EU;
- product manufacturers who place an AI system on the market or put it into service an AI system within the EU together with their product and under their own name or trademark;

- authorized representatives of AI systems where such providers are not established in the EU; and
- affected persons or citizens located in the EU.

The AI Act is subject to a final linguist check by lawyers, which is expected to take place in April 2024. This is essentially a validation of the language in the final text of the AI Act to ensure that language translations do not lose the legal meaning set out in the original text. It will also need to be formally endorsed by the European Council. As such, it is expected to be finally adopted before the end of the EP's legislature in June 2024.

The AI Act will enter into force 20 days after its publication in the Official Journal. It will be fully applicable 24 months after its entry into force. However, certain provisions will come into force and need to be complied with sooner.

Timeline and Transition Period

After the Council of the European Union (the "*Council*") formally endorses the AI Act, it will be published in the Official Journal and enter into force 20 days later. The AI Act provides various transition periods for specific requirements, including:

- **Prohibited AI practices**: The transition period for prohibited AI practices, including certain uses of General Purpose AI ("*GPAI*") systems, is **6 months**;
- **High-risk AI practices**: The transition period for the requirements for high-risk AI systems is **24 months**; and
- **General-purpose AI**: The transition period for the requirements on general-purpose AI models (as defined below) and GPAI models that pose systemic risk ("*GPAI-SR***"**) is **12 months**.

No fines will be imposed for any violation of the GPAI requirements for a further 12 months, creating a *de facto* additional grace period.

Pre-existing AI Systems

After the transition periods have passed, the AI Act will also apply to AI systems that are already available on the EU market if, after this transition period, a substantial modification is made to the AI system. The AI Act will apply to pre-existing GPAI models after 36 months, regardless of whether they are subject to substantial modifications.

<u>Scope</u>

Definition of AI Systems

The AI Act applies to *AI systems*. An "*AI system*" is defined in the text of the Act as "*a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives*, *how to* generate outputs such as *predictions, content*, recommendations, or decisions *that can influence physical or virtual environments."* The term aligns both with the updated OECD definition of AI systems issued in 2023 as well as the definition set out by the Biden administration in its Executive Order 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence published in October 2023.

Geographic Scope and Scope of AI Systems caught by the AI Act

The AI Act has extra-territorial scope. This means that organizations outside the EU will have to comply with the law in certain specified circumstances as well as those within the EU. The Act applies to providers, deployers, and users of AI systems.

The AI Act applies to:

- providers placing AI systems or models on the market in the EU or putting into service AI systems or placing on the market general-purpose AI models in the EU, irrespective of whether those providers are located within or outside the EU;
- deployers of AI systems that have their place of establishment in or who are located within the EU;
- providers and deployers of AI systems that have their place of establishment or who are located in a third country in situations where the output produced by the AI system is used in the EU;
- importers and distributors of AI systems into or within the EU;
- product manufacturers who place an AI system on the market or put it into service an AI system within the EU together with their product and under their own name or trademark;
- authorized representatives of AI systems where such providers are not established in the EU; and
- affected persons or citizens located in the EU.

It is therefore extremely wide-reaching. It is noteworthy that the AI Act applies to the outputs of AI systems used within the EU, even if the AI providers or deployers are themselves not located in the EU.

Tiered Approach to Regulating AI Systems

The AI Act will prohibit certain AI systems in the EU. It also sets out various categories or tiers of AI systems that each carry different levels of obligations as well as potential fines for non-compliance.

Prohibited AI Practices

Certain AI practices that are deemed to pose an unacceptable risk to individuals' rights will be banned. These prohibited AI practices include:

- using AI to exploit the vulnerabilities of individuals;
- using AI to manipulate individuals using subliminal techniques;
- social scoring (with limited exceptions);
- predicting the likelihood of an individual committing a criminal offense based solely on profiling of their personality traits and characteristics;
- the use of biometric identification systems in publicly accessible spaces for law enforcement (with limited exceptions);
- the use of emotion recognition within the workplace and educational institutions; and
- untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases.

The last of these prohibitions, in particular, may have wide-reaching impacts for existing trained models that have incorporated these practices already as well as for the necessary engineering approach going forward.

High-Risk AI Systems

The AI Act places several detailed obligations on what it categorizes as "*high-risk AI.*" Examples of high-risk AI uses include use of AI systems in critical infrastructure, education and vocational training, employment, essential private and public services (such as healthcare and banking), certain systems in law enforcement, migration and border management, justice, and democratic processes (for example, influencing elections).

For high-risk AI systems, organizations must assess and reduce risks, maintain use logs, be transparent (see more on transparency below) and accurate, and ensure human oversight. Individual citizens will have a right to submit complaints to the relevant market surveillance authority and to receive explanations about decisions based on high-risk AI systems that affect their rights.

Provisions Relating Specifically to General-Purpose AI

The final text of the AI Act includes a new regime for providers of GPAI models . The AI Act defines a GPAI model as: *"an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are released on the market."*

As indicated in our December briefing, GPAI models will be subject to its own risk-based, two-tier approach, with a set of requirements that apply to all GPAI models and more stringent requirements applicable only to GPAI-SR. Separate requirements apply to GPAI *systems* (i.e., AI systems based on GPAI models). GPAI systems can qualify as high-risk AI systems, if they can be used directly for at least one purpose that is classified as high risk.

The providers of all GPAI models must:

- create technical documentation of the GPAI model and provide this to the AI Office or competent local supervisory authority upon request;
- create documentation for third parties who use the GPAI model to create their own AI systems;
- implement a policy to respect EU copyright law and specifically text and data mining ("*TDM*") opt-outs (see application of copyright law to AI systems and rights to opt-out below); and
- make available a summary about the content used to train the GPAI model.

GPAI with Systemic Risk

Providers of GPAI-SR will be subject to additional requirements. GPAI models pose a systemic risk if, for example, they have high impact capabilities in the sense that the cumulative amount of compute used for their training measured in FLOPS is greater than 10^25. This would be a lower threshold than the 10^26 FLOPS threshold for the reporting obligation under the U.S. Executive Order on AI, which we reported in our previous **alert**.

In addition to the requirements outlined above, providers of GPAI-SR models must:

- Perform model evaluation to identify and mitigate systemic risk (e.g., negative effects on democratic process and dissemination of illegal, false, or discriminatory content), and continuously assess and mitigate such systemic risk;
- Assess and mitigate possible systemic risks at an EU level, which may stem from the availability and/or use of the GPAI model that poses systemic risk;
- Report serious incidents to the AI Office and the competent local supervisory authority; and
- Ensure an adequate level of cybersecurity for the GPAI model that poses systemic risk and physical infrastructure.

Regulation of GPAI models

Providers of both GPAI and GPAI-SR models may rely on a code of practice **to demonstrate compliance** with the AI Act requirements, until a harmonized standard is published. Providers of GPAI should furthermore be able to demonstrate compliance using alternative adequate means, if codes of practice or harmonized standards are not available, or they choose not to rely on those.

The AI Office will facilitate the drawing up of a code of practice and will invite providers of GPAI models, competent national authorities, and other relevant stakeholders (e.g., academia, civil society organizations, industry groups) to participate. Providers of GPAI models may also draft their own code of practice. Completed codes of practice will have to be presented to the AI Office and AI Board for assessment, and to the EC for approval. The EC can decide to give any code of practice general validity within the EU, e.g., allowing providers of GPAI models to rely on a code of practice prepared by another provider of a GPAI model.

If no code of practice has been completed and approved when the GPAI-requirements become effective (i.e., 12 months after the GPAI-chapter of the AI Act becomes effective, expected to be around the end of Q2 2025), the EC may adopt common rules for the implementation of the GPAI and GPAI-SR obligations by adopting an implementing act.

Deepfakes and Chatbots

Crucially, the AI Act specifically requires that (save for certain public interest exemptions) artificial or manipulated images, audio, or video content ("*deepfakes*") need to be clearly labeled as such. This is particularly important in a year when so many elections are taking place given the potential influencing power of such deepfakes. Similarly, when AI is used to interact with individuals (e.g., via a chatbot), it must be clear to the individual that they are communicating with an AI system.

Application of Copyright Law to AI Systems and Rights to Opt-Out

The AI Act obliges GPAI providers to implement a policy to respect EU copyright law. Copyright law applies to the field of AI, both to use of copyrighted works for *training purposes* and the potential infringing *outputs* of the GPAI models.

The AI Act includes a training data transparency obligation, which initially related to copyrighted training data but covers all types of training data in the final version. Providers of GPAI models have to make publicly available a sufficiently detailed summary of the content used for training, which should be generally comprehensive to facilitate parties with legitimate interests, including copyright holders, to exercise and enforce their rights under EU law, but also take into account the need to protect trade secrets and confidential business information. The AI Office is due to provide a summary template which will give more insight here as to what will be expected.

For use of copyrighted works for *training purposes*, the AI Act explicitly mentions that GPAI providers must observe opt-outs made by rights holders under the Text and Data Mining or TDM exception of Art. 4(3) of **Directive (EU) 2019/790.** This exception entails that where an opt-out has been effectively declared in a machine-readable form by an organization, the content may not be retrieved for AI training.

This provision clarifies that the TDM exception also applies to the use for training GPAI, but it leaves a variety of practical uncertainties open (e.g., technical standards for opt-out, scraping of content from websites where the rights holder is unable to place an opt-out, declaring an opt-out after the AI has already been trained with the data, and evidentiary challenges when enforcing rights in training data). The final text does set an expectation for providers of GPAI to use of "state of the art technologies" to respect opt-outs. It is noteworthy that a recital underlines that any provider *placing* a GPAI model on the EU market must be copyright compliant in the meaning of this provision, even indicating that AI training conducted outside the EU must observe TDM opt-outs.

As to potential copyright issues relating to *the output* of the AI models, the AI Act itself does not provide clarifications as to the copyright position. It should be noted that there are already a number of litigations in play regarding this area both in Europe and beyond. Therefore, many follow-up questions remain outstanding, such as whether prompts likely to cause infringing outputs should be blocked from processing, how to reliably assess AI output under copyright law (e.g., as a parody or pastiche), the allocation of liability between provider and user, notice and takedown procedures, etc.

The bottom line remains that the existing copyright frameworks within the EU and the accompanying technical side do not yet have a tailor-made response to copyright issues related to training data and the impact on the usability of the respective AI system. Over time, courts or private actors may shape solutions both within the EU and globally.

Limited Exemptions for Free and Open-Source AI Models

The AI Act contains exceptions for free and open-source AI models. The requirements of the AI Act do not apply to AI systems released under free and open source licenses except:

- if they are placed on the market or put into service as high-risk AI systems;
- if they qualify as a prohibited AI practice; or
- if the transparency requirements for deepfakes or chatbots apply to the system (see above).

Governance and Enforcement

There are four key aspects of future governance under the AI Act:

- *National competent authorities*will supervise and enforce the AI Act's application and implementation regarding conformity of high-risk systems. Each Member State must establish or designate at least one notifying authority (responsible for conformity assessment bodies and their monitoring) and one market surveillance authority (responsible for ex-post monitoring).
- *The EC and the AI Office*:The EC established a dedicated AI Office in February 2024, which is tasked with central oversight and enforcement of the rules regarding GPAI,

facilitating those requirements (e.g., by issuing template documents), and developing EU expertise and capabilities in the field of AI. In addition, the EC is responsible for the overall framework of the AI Act, including evaluating new AI technologies and updating the criteria for qualifying as GPAI models that pose systemic risk or high-risk AI over time.

- *The Scientific Panel:* A scientific panel of independent experts will be formed to assist the AI Office. The panel will have an advisory role, contributing to the development of evaluation methodologies for GPAI and advising on the selection and impact of GPAI. The panel will monitor safety issues in the market and will launch qualified risk alerts to the AI Office that may trigger investigations.
- *The AI Board*: The AI Board will consist of one representative from each EU Member State and will serve as a coordination platform and advisory body to the EC and is tasked with supporting a consistent application of the AI Act across EU Member States by developing standards and issuing guidance.

Fundamental Rights Impact Assessments Are Required, But Not Always

The AI Act requires a fundamental rights impact assessment to be conducted for high-risk AI systems, but only by public authorities, or by private actors when they use AI systems for credit scoring or for risk assessment and pricing in relation to life and health insurance. A fundamental rights impact assessment must include:

- a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose;
- a description of the period of time and frequency in which each high-risk AI system is intended to be used;
- understanding the categories of natural persons and groups likely to be affected by the use of the AI System in the specific context;
- understanding the specific risks of harm likely to impact the identified categories of persons or group of persons, taking into account the information given in the provider's instructions;
- a description of the implementation of human oversight measures, according to the instructions of use; and
- the measures to be taken if these risks materialize, including internal governance and complaint mechanisms.

Where the deployer is already required to carry out a data protection impact assessment under the EU General Data Protection Regulation ("*GDPR*"), the fundamental rights impact assessment must be conducted in conjunction with the data protection impact assessment.

Compliance with this obligation will be facilitated by the AI Office, which has been tasked with developing a template for the fundamental rights impact assessment.

Enforcement and Increased Penalties

The maximum penalties for non-compliance with the AI Act were increased in the political agreement on the EU AI Act reached in December. There are a range of penalties and fines depending on the level of non-compliance. At their highest level, an organization can be fined an astounding EUR 35 million or 7% of global annual turnover.

As with the GDPR, these levels of fines mean that organizations have a strong financial imperative to comply with the AI Act's provisions and with ethical and societal rationales.

Interaction with Data Protection Laws

Since the first draft of the AI Act, it was made clear that it would act as a "top up" of the GDPR in relation to personal data and that the GDPR remains applicable. The final text clarifies that both individuals and supervisory authorities keep all their rights under data protection laws, such as the GDPR and the ePrivacy Directive, and that the AI Act does not affect the responsibilities of providers and deployers of AI as controllers or processors under the GDPR. The responsibilities under the GDPR are relevant because many of the risk-management obligations under the AI Act are similar to obligations that already exist under the GDPR. The AI Act, however, has a far broader scope and will also apply if the AI system:

- is trained with *regular*data (i.e., not personal data subject to the GDPR);
- is trained with personal data not subject to GDPR; or
- if the provider bringing the AI system on the EU market does not qualify as a "controller" under GDPR.

As explained in detail in one of our previous **alerts**, many risk-management obligations under the AI Act cover similar topics as those under the GDPR. The obligations under the AI Act, however, are more detailed and wider in scope (applying to all data). By way of example:

- the AI Act's requirement to implement a risk-management system shows many similarities to the GDPR's requirement to conduct a data protection impact assessment (DPIA);
- the AI Act's requirement to implement data governance measures, including the use of appropriate datasets, is similar to the GDPR's requirement to ensure the fair and lawful use of personal information; and
- the AI Act's requirement to ensure appropriate human oversight, proportionate to the risk posed by the AI system, is similar to the GDPR's prohibition on automated decision making (with limited exceptions).

Controllers under the GDPR who currently train (or further train) AI systems with personal data or use AI systems processing personal data will therefore be able to leverage their GDPR compliance efforts toward complying with the AI Act's risk management obligations.

Currently, it appears that the only specific requirement in the AI Act that fully overlaps with the GDPR is the right granted to individuals to an explanation for decisions based on high-risk systems that impact the rights of individuals (see below).

Limited Rights for Individuals

The initial draft of the AI Act did not bestow any rights directly on individuals. The final text changes this, by granting individuals the right to:

- *Obtain an explanation of a decision* made by a deployer of high-risk AI system on the basis of the output from such high-risk AI system, where the decision has legal effects or similarly significantly affects that person. The individual is in this case entitled to obtain a clear and meaningful explanation on the role of the AI system in the decision-making procedure and the main elements of the decision taken. The AI Act does not shed much light on the exact content of such explanation, but merely indicates that it should be clear and meaningful and should provide a basis for affected individuals to exercise their rights. This right is broader than the right to an explanation of an automated decision under the GDPR. Whereas the right under the GDPR is limited to decisions based solely on automated processing, the right under the AI Act extends to all decisions taken based on the output of a high-risk AI system (i.e., also including human decisions based on AI outputs); and
- *Complain to a supervisory authority*if the individual considers that there is an infringement of the AI Act.

The AI Act and National Security

The AI Act includes an exemption for AI systems that exclusively serve military, defense, or national security purposes.

The AI Act does "*not apply to areas outside the scope of EU law*" and in any event should not affect member states' competences in national security, "*regardless of the type of entity entrusted by the Member States to carry out tasks in relation to those competences.*" The consolidated text clarifies that only if AI systems *exclusively* serve military, defense, or national security purposes, the AI Act does not apply. If an AI system is used for other purposes as well (e.g., civilian or humanitarian), or gets repurposed at a later stage, providers, deployers, and other responsible persons or entities must ensure compliance with the regulation.

The exemption, however, remains unclear in the sense that the notion of "national security" is not clearly defined under EU law, and Member States apply different concepts and interpretations. To rely on the exemption for national security purposes other than military or defense, companies need to be mindful to ensure the respective purpose is indeed *exclusively* a "national security" use case in each Member State where an EU nexus exists.

The recitals of the AI Act suggest that any use for "public security" would be distinct from a "national security" purpose, which appears inconsistent with the goal not to interfere with member state competences and to align the AI Act with other recent EU legislation like the Data Act, which exempts national security and public security purposes altogether.

The AI Act indeed foresees specific derogations with regard to public security. For example, it recognizes the interests of law enforcement agencies to quickly respond in duly justified situations of urgency for exceptional reasons of public security by using high-risk AI tools that have not passed the conformity assessment.

Looking at the broader implications of the AI Act in the area of national security, it may have an indirect impact on how AI tools will be viewed by member state authorities regulating their national security interests. For example, the AI Act may help by framing the undefined notion of AI included in the current EU framework regulation for screening of foreign direct investments (the EU Commission only recently published a proposal of a new foreign investment screening regulation, *see our client alert here)*. According to this framework, member states may take critical technologies, including artificial intelligence, into account when determining whether an investment is likely to affect security or public order.

Allocation of Responsibilities Across the AI Value Chain

Another key aspect that the AI Act includes is the allocation of compliance obligations along the AI value chain. All draft versions of the AI Act provided a mechanism where the obligations of the AI provider automatically transfer to certain deployers or to other operators. The final provides that any distributor, importer, deployer, or other third party shall be considered a provider of a high-risk AI system for the purposes of the AI Act, and shall be subject to the respective provider obligations, in certain defined circumstances, namely if:

- they put their name or trademark on a high-risk AI system already placed on the market or put into service (The AI Act does, however, clarify that the parties may have contractual arrangements in place that allocate the obligations otherwise between them, which will likely only refer to their internal relationship and not affect their external relationships);
- they make a substantial modification to a high-risk AI system in a way that it remains a high-risk AI system; or
- they modify the intended purpose of an AI system, including a GPAI system, which has not been classified as high-risk and has already been placed on the market or put into service in such manner that the AI system becomes a high-risk AI system.

In these circumstances, the provider that initially placed the relevant AI system on the market or put it into service shall no longer be considered a provider of that specific AI system for purposes of the AI Act. In essence, all AI Act obligations in relation to the modified/rebranded AI system will switch to the new provider.

This would apply even where, for example, a non-compliance of the AI system with the AI Act was already triggered by the original provider. Thus, the new provider may be responsible for compliance shortfalls of the original provider.

The original provider shall, however, closely cooperate and make available necessary information and provide reasonably expected technical access and other assistance required for new provider to fulfill its obligations under the AI Act.

The AI Act also retains the further EP proposal to obligate providers of high-risk AI systems and third parties that supply AI systems, tools, services, components, or process to such providers for integration into the high-risk AI system to specify details for their cooperation by written agreement. The terms of that agreement must allow the provider of the high-risk AI system to fully comply with its obligations under the AI Act.

In addition to the cooperation obligations, the final text stipulates specific technical documentation requirements for GPAI models to facilitate integration into downstream AI systems.

This area, as with any value chain proposition, needs careful forethought, both in the adoption and use of AI within one's own systems or for original providers allowing such use. Contractual provisions will be key here.

What's Next?

As mentioned above, the AI Act is expected to be formally endorsed by the Council before the end of the European Parliament's legislature in June 2024. The AI Act will then be subject to various transition periods (see Timeline and Transition Periods above).

Click Here for the Original Article

California Pay Data Reporting is Due May 8, 2024 (Now with New Requirements)

California requires private employers of 100 or more employees and/or 100 or more workers hired through labor contractors to annually report pay, demographic, and other workforce data to the Civil Rights Department ("CRD").

The CRD has published "important announcements" regarding changes to this year's reporting requirements, including the following:

- **New data fields for remote workers**: Employers must now report information regarding the extent to which its workforce is remote during the "Snapshot Period" (i.e., a single pay period of the employer's choice between October 1 and December 31, 2023). Specifically, the CRD added three new reporting fields: (1) the number of remote employees located within California; (2) the number of remote employees located outside of California; and (3) the number of employees that do not work remotely. For purposes of this reporting, the CRD defines a "remote worker" as "[a] payroll or labor contractor employee who is entirely remote, teleworking, or home-based, and has no expectation to regularly report in person to a physical establishment to perform work duties." Therefore, hybrid employees are not considered "remote" for these purposes.
- **Race, ethnicity, sex for Labor Contractor Employee Reports**: Reporting "unknown" race/ethnicity or sex of a labor contractor employee is no longer permitted. According to the CRD, employee self-identification is the preferred method of identifying race/ethnicity and sex information; however, if an employee declines to state their sex or voluntarily provide their race/ethnicity, the employer should report using current employment records, other reliable records or information, or observer perception. When a reporting entity must rely on observer perception, the CRD encourages specifying this through clarifying remarks (e.g., "The race/ethnicity of [*number*] individuals in this grouping is being reported based on observer perception.").
- **Filing deadline**: Reports are due by May 8, 2024. Unlike last year's reporting period, it does not appear that the CRD will be accepting or granting any pay reporting submission deferral requests.

Employers are well-advised to use this year's reporting templates and consult the updated User Guide available here. California employers also may wish to consult the CRD's Updated FAQs and/or consult with counsel in advance of the May 8, 2024 deadline.

Click Here for the Original Article

Whistleblower Protection Laws Do Not Apply Outside the United States

Tayo Daramola is a Canadian citizen who resided in Montreal at all relevant times and who worked for Oracle Canada, a wholly owned subsidiary of Oracle Corporation (a California-based company). Daramola's employment agreement stated that it was governed by Canadian law. During his employment, Daramola, who worked remotely, conducted business and collaborated with colleagues in Canada and the United States and was assigned as lead project manager for the implementation of an Oracle product at institutions of higher education in Texas, Utah, and Washington. In time, Daramola came to believe that by offering this product, Oracle was committing fraud, and he reported same to Oracle and the SEC. Eventually, Daramola resigned his employment based upon his "unwillingness to take part in fraud."

He then filed a lawsuit in federal court in California, claiming violations of the Sarbanes-Oxley Act and the Dodd-Frank Act, as well as the California whistleblower protection act, Cal. Lab. Code § 1102.5. The district court dismissed the lawsuit after twice giving Daramola leave to amend his complaint. The Ninth Circuit affirmed dismissal of the action, holding that the anti-retaliation provisions of the state and federal statutes at issue did not apply to Daramola, a Canadian citizen working out of Canada for a Canadian subsidiary of a U.S.-based parent company.

Click Here for the Original Article