JANUARY 2024

CLEARSTAR®

SCREENING COMPLIANCE UPDATE

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

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

CLICK FOR PAST UPDATES

CLEARSTAR®

TABLE OF CONTENTS

SCREENING COMPLIANCE UPDATE | JANUARY 2024

Clearstar is happy to share the below industry related articles written by subject matter experts and published on the internet in order to assist you in establishing and keeping a compliant background screening program.

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENT

CFPB issues two new FCRA advisory opinions on background screening reports and disclosure of credit files to consumers

On January 11, 2024, the Consumer Financial Protection Bureau (CFPB) issued two new advisory opinions: Fair Credit Reporting; Background Screening and Fair Credit Reporting; File Disclosure. The advisory opinions are part of the CFPB's ongoing efforts to clean up what the CFPB describes in its press release as allegedly "sloppy" credit reporting practices and ensure credit report accuracy and transparency to consumers. As a reminder, advisory opinions are interpretive rules that provide guidance on the CFPB's interpretation of a particular law or regulation.

The Biden Administration kicked off 2023 by issuing the "Blueprint for a Renter Bill of Rights" and directing the CFPB and Federal Trade Commission (FTC) to take actions in furtherance of those principles. In February, the CFPB and FTC issued a request for information on background screening in connection with rental housing. In July, the FTC issued a blog post reminding landlords, property managers, and other housing providers of their obligation under the Fair Credit Reporting Act to provide notice of adverse action when information in a consumer report leads them to deny housing to an applicant or require the applicant to pay a deposit that other applicants would not be required to pay. In November, the CFPB released two reports concerning tenant background checks. "Consumer Snapshot: Tenant Background Checks" discusses consumer complaints received by the CFPB that relate to tenant screening by landlords and "Tenant Background Checks Market" looks at the practices of the tenant screening industry. The CFPB has previously addressed the issues of accurate credit reporting and investigating credit report disputes in its supervisory highlights.

Background Checks

In the first advisory opinion, the CFPB addresses the provision of background check reports. Background checks are used by landlords and employers to make rental and employment determinations, respectively. Background check reports prepared by employment and tenant screening companies often contain information compiled from several sources about a consumer's credit history, rental history, employment, salary, professional licenses, criminal arrests and convictions, and driving records. The CFPB advisory says prior research has determined that background check reports often contain false or misleading information that may adversely affect an individual's housing or employment. In 2021, the CFPB issued an advisory opinion that it was unreasonable for consumer reporting agencies (CRAs) to use name-only matching (matching records to a consumer by first and last name without any other identifying information).

The current advisory opinion highlights that CRAs, covered by the Fair Credit Reporting Act (FCRA), must "follow reasonable procedures to assure maximum possible accuracy" under Section 607(b). Specifically, the CRA's procedures should:

1. Prevent the reporting of public record information that has been expunged, sealed, or otherwise legally restricted from public access;
2. Ensure disposition information is reported for any arrests, criminal charges, eviction proceedings, or other court filings that are included in background check reports; and
3. Prevent the reporting of duplicative information.

The advisory opinion further reminds consumer reporting companies that they may not report outdated negative information, such as a criminal charge that does not result in a conviction, for periods longer than permitted under FCRA section 605(a). While no time limit applies to reporting disposition information on criminal convictions, an arrest with no conviction ends seven years after the arrest date and subsequent events do not restart the reporting period applicable to the arrest. The CFPB further highlighted its settlement with TransUnion related to furnishing tenant screening reports without including available disposition information for the eviction proceedings.

CRA Disclosure of Credit Files

In the second advisory opinion, the CFPB addresses the consumer reporting agencies' disclosure obligations to deliver complete files to consumers upon request. In the advisory opinion, the CFPB clarifies the consumer reporting agencies' obligation, pursuant to Section 609(a) of FCRA, upon the consumer's request, to "clearly and accurately" disclose "all information in the consumer's file at the time of the request." Relying on a Third Circuit holding in *Kelly v. RealPage, Inc.*, 47 F.4th 202, 221 (3rd Cir. Aug. 24, 2022), the CFPB further emphasizes that consumers do not need to use specific language (such as "complete file" or "file") in their request to trigger a consumer reporting agency's file disclosure requirement under Section 609(a).

Specifically, the consumer reporting agency must provide consumers the following:

1. At least one free file disclosure annually and in connection with adverse action notices and fraud alerts;
2. Consumer's complete file with clear and accurate information that is presented in (i) a way an average person could understand and (ii) a format that will assist consumers in identifying inaccuracies, exercising their rights to dispute any incomplete or inaccurate information, and understanding when they are being impacted by adverse information; and
3. All sources for the information contained in consumers' files, including both the originating sources and any intermediary or vendor sources, so consumers can identify the source and correct any misinformation (noting that only providing summarized information would not be compliant).

However, Section 609(a) does not require disclosure of any credit score, risk score or predictor.
This new file disclosure guidance aligns with the CFPB's other efforts to ensure consumers have access to their data in Personal Financial Data Rights rulemaking and the Section 1034(c) advisory opinion.

As we previously blogged, the CFPB also has launched an FCRA rulemaking. We will continue to monitor any CFPB developments related to FCRA.
CLICK HERE.

Biden Administration Announces Actions Aimed at Advancing Pay Equity for the Federal Workforce and Federal Contractor Employees

The Biden Administration announced actions to support the equal pay principles set forth by Executive Orders 14035 and 14069. These actions will impact federal contractors and subcontractors who will be required to disclose pay ranges in certain job postings and prohibited from relying on salary history information when setting pay. Further, these actions will impact federal agencies who will be prohibited from considering current or past pay when determining the salary of federal employees.
CLICK HERE.

Class Action Areas Drive EEOC's Strategic Enforcement Plan for 2024 – 2028

Late last year, the EEOC quietly announced its most recent Strategic Enforcement Plan, covering 2024–2028. To no surprise, the EEOC has indicated that it will implement a concerted effort to focus its resources on employment practices that often result in class and collective action lawsuits. More specifically, the EEOC announced the following "subject matter priorities" for the next four years:

- **"Eliminating Barriers in Recruitment and Hiring"** (including use of artificial intelligence for hiring, apprenticeship/internship programs, online-focused application processes, screening tools for hiring—such as pre-employment tests and background checks, and the underrepresentation of women and workers of color in industries such as manufacturing, tech, STEM, and finance, for example);
- **"Protecting Vulnerable Workers and Persons from Underserved Communities from Employment Discrimination"** (including immigrant workers, persons with mental or developmental disabilities, temporary workers, older workers, and workers traditionally employed in low-wage jobs);
- **"Addressing Selected Emerging and Developing Issues"** (including the use of qualification standards or other policies that negatively affect disabled workers, protecting workers affected by pregnancy, childbirth or related medical conditions, preventing discriminatory bias towards religious minorities or LGBTQIA+ individuals, and the use of artificial intelligence or automated recruitment tools for hiring);

- **"Advancing Equal Pay for All Workers"** (including a focus on employer policies that prevent or attempt to limit workers from asking about pay, inquiring about applicants' prior salary histories, or prohibiting workers from sharing their compensation with coworkers);
- **"Preserving Access to the Legal System"** (including the use of overly broad releases or nondisclosure agreements, the implementation of unlawful mandatory arbitration provisions, and any failure to keep records required by statute or EEOC regulations); and
- **"Preventing and Remedying Systemic Harassment."**

The EEOC has indicated that it will focus on Charges that touch on the above topics while also intentionally prioritizing systemic enforcement actions and impact litigation to eradicate what it perceives to be discriminatory employment practices. As demonstrated briefly above, the EEOC has a keen interest in scrutinizing artificial intelligence and mass hiring practices via automatic recruitment tools, in addition to a renewed focus on employment practices that could have an adverse impact on those with intellectual or health-related disabilities, among other things. This could directly lead to an increase in Commissioner Charges, systemic investigations, pattern or practice lawsuits, and class action litigation regarding the topics listed in its Strategic Enforcement Plan.

Employers should be vigilant in monitoring these key areas of risk related to the EEOC's new Strategic Enforcement Plan, as EEOC investigations can quickly escalate to regional or even nationwide systemic investigations and corresponding litigation.
CLICK HERE.

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

New Pennsylvania Legislation and Philadelphia Ordinance Amendment Tackle Pardoned Convictions, Expunged Records, and Negligent Hiring Liability

Pennsylvania and Philadelphia recently enacted changes that impact employer criminal background screening.

State Law
Enacted on December 14, 2023, and effective February 12, 2024, Pennsylvania's House Bill No. 689 amends Pennsylvania law relating to the expungement of certain criminal record information and employer immunity when hiring individuals with expunged records.

First, the legislation immunizes employers from liability for any claim related to the effects of expunged records or the lawful use of criminal record history information when an applicant voluntarily discloses an expunged conviction. This helps clarify a potential ambiguity under existing state law regarding whether an employer still might face negligent hiring liability for hiring an individual with an expunged criminal record where the individual goes on to commit some misconduct, such as injuring a third party. Previously, a negligent hiring lawsuit might contend that if the employer learned about an expunged criminal record by means other than a formal background check or official court records, the employer should have used the record to disqualify the person, and by not doing so, was negligent. Such a stance would seemingly be contrary to the purpose behind criminal record expungement, and the new legislation seems intended to prevent such an incongruous argument from surviving dismissal.

Second, the law extends the availability of automatic expungements to pardons. The law requires that the Pennsylvania Board of Pardons, which administers pardons, to notify the Administrative Office of Pennsylvania Courts (AOPC) on a quarterly basis of any pardons, and then requires the AOPC to notify the relevant Court of Common Pleas to order the record expunged. Under the law as amended, criminal history record information that has been expunged or granted limited access cannot be used by private entities for employment, housing, or school matriculation purposes, unless required by federal law. If the law works as intended, employers should simply not see the pardoned cases because they are supposed to be unavailable to the public. However, given the number of required steps in the process and different entities involved, it is not inconceivable that a candidate may believe an offense has been expunged, when it fact it remains available in the public record. Moreover, several pieces of this process remain unclear, such as how quickly the AOPC will act upon receipt of information from the Board of Pardons, whether individuals will be notified that their pardoned convictions were expunged, and whether the court docket will be changed to reflect a pardon status while expungement is in process.

Third, the law expands eligibility for Pennsylvania's pre-existing limited access status for criminal records. Now, certain individuals who are free from conviction for seven years and otherwise meet requirements can petition for limited access; previously, the minimum threshold was 10 years. The law also clarifies categories of offenses that are and are not eligible for limited access petitions.

Notably, this statewide legislation does not amend the existing requirements on an employer's general use of criminal record history.[1] Under existing law, Pennsylvania employers generally are required to use only job-related misdemeanor and felony convictions in making hiring decisions.

Philadelphia Ordinance
Philadelphia employers are subject to additional restrictions and procedural requirements under Philadelphia's Fair Criminal Record Screening Standards Ordinance. For its part, Philadelphia weighed in by enacting an amendment to that ordinance specifically addressing employer use of convictions subject to "exoneration." The city ordinance, effective January 19, 2024, defines "exoneration" as reversing or vacating a conviction by pardon, acquittal, dismissal or other post-conviction re-examination of the case by the court or other government official, and generally prohibits employers from denying employment based on convictions subject to "exoneration" as so defined.

To prepare for the January and February effective dates of the laws, employers in Pennsylvania may want to ensure that they have considered how to handle situations in which a candidate identifies that an offense has been expunged, pardoned, granted limited access or subject to other post-conviction relief before potentially denying employment based on such a record.

CLICK HERE.

Reminders About California's Fair Chance Act

California's Fair Chance Act also known as the "Ban the Box" law took effect in January 2018. It generally prohibits employers with five or more employees from asking about your conviction history before making you a job offer. In 2021, California's Civil Rights Department (formerly the Department of Fair Employment and Housing) announced new efforts to identify and correct violations of the Fair Chance Act. Since then, the Civil Rights Department has stepped up enforcement of the statute. As such, it is vital for covered employers to understand the requirements under the law.

Covered Employers
Public and private employers with five or more employees are covered by the law. This includes union hiring halls, labor contractors, temporary employment agencies, and client employers.

Requesting Background Checks
Covered employers may not ask applicants about their criminal history until after a conditional offer is extended. However, even after a conditional offer, employers may not ask about or consider information about the following:

- An arrest that did not result in a conviction.
- Referral to or participation in a pretrial or posttrial diversion program.
- Convictions that have been sealed, dismissed, expunged, or statutorily eradicated.

Steps for Rescinding a Job Offer
Under the law covered employers must take specific steps if they want to rescind a conditional job offer based on an applicant's criminal history.

1. Conduct an individualized assessment.
2. Provide notification in writing that the applicant's criminal history disqualifies the applicant from the position. The notice must also provide the conviction(s) that disqualify the applicant.
3. Provide a copy of the conviction history report to the applicant.
4. Provide the applicant 5 business days to respond to the preliminary decision to rescind.
5. Consider any response from the applicant.
6. Provide final notice in writing about disqualification.

The Civil Rights Department has sample forms available on its website.
CLICK HERE.

Florida Law Imposes Additional E-Verify Requirements for Private Employers

Further Hiring Requirements for Private Employers
A. Overview of Senate Bill 1718 (**"SB1718"**)

Earlier this year, the State of Florida enacted a law that continues to have significant implications for employers across the Sunshine State. On May 10, 2023, Governor Ron DeSantis signed into law SB1718, now **Section 448.095, Florida Statutes** ("**Section 448.095**"), which requires private employers with 25 or more employees to use E-Verify for new hires—a measure aimed at combating illegal immigration into the state. This requirement became effective as of July 1, 2023.

B. Law Prior to SB1718

Since 2021, Florida law required every public agency, contractor, and subcontractor to use the E-Verify system to authenticate the work status of recent hires. Under such law, a contract between a public agency and a contractor and/or subcontractor must contain language that any new hires will be validated through E-Verify. This requirement applies to all contractors or subcontractors, regardless of size and employee headcount, under contract with a public agency. Notably, if a contractor enters into a contract with a subcontractor, the subcontractor must provide the contractor with an affidavit stating that the subcontractor does not employ, contract with, or subcontract with an unauthorized alien.

C. SB1718 Broadens Existing Law to Include Private Employers

The passing of SB1718 does not change the above requirements. Instead, the new law broadens the mandate to include all private employers with at least 25 employees, regardless of whether such private employers are under contract with a public agency. This requirement for private employers only applies to employees hired after July 1, 2023. Independent contractors are not subject to the requirements of Section 448.095.

Private employers have expressed confusion regarding the boundaries of the new law. It was unclear whether all 25-plus employees had to be based in Florida and also, whether out-of-state employers with remote workers based in Florida had to comply with the requirements of Section 448.095.

To clarify such confusion, the Florida Department of Revenue recently issued **guidance** on the issue, opining that according to Section 448.095, private employers with 25 or more employees performing services in Florida must certify the eligibility of their employees performing services in Florida (emphasis added). This development makes it clear—the E-Verify mandate applies to employees performing services in Florida, whereas such mandate does not apply to employees not performing services in the state.

Overview of the E-Verify System
Operated by the United States Department of Homeland Security, E-Verify is an online system that allows employers to verify the employment eligibility of new employees by comparing their information with government records. Mainly, the E-Verify system cross-references the social security number provided by the employee with the records of the Social Security Administration.

Despite Section 448.095, existing employer I-9 requirements remain in place. Employees hired before July 1, 2023 remain subject to all I-9 mandates, however, their information does not need to be entered into the E-Verify system.

How to Register in E-Verify
Florida private employers with over 25 or more employees must utilize E-Verify to authenticate all new hires. Employers can **enroll online** and find additional information on the **E-Verify website**.

Enforcement of Section 448.095
Enforcement for covered employers began on July 1, 2023. If the Florida Department of Economic Opportunity ("**DEO**") determines an employer has failed to comply with the E-Verify requirements of Section 448.095, DEO will send such employer a notification and the employer will have 30 days to correct the noncompliance. If three violations occur in a 24-month period, a fine of $1,000 per day may be imposed. Also, other civil and criminal penalties may be imposed on a case-by-case basis, including suspension or revocation of state licenses, permits, registrations, among others.

Implications on Florida's Business Community
The requirements of Section 448.095 increase the administrative responsibilities on employers. The expansion of the new law to include private employers with 25 or more employees requires thousands of business to adjust their customary procedures for onboarding new hires. With steep penalties for non-compliance, employers and their advisors must educate internal stakeholders of the requirements of Section 448.095. Those businesses contracting with government must be especially vigilant as there is no minimum number of employees to require the use of E-Verify.
CLICK HERE.

Washington D.C. is Set to Join the Trend Toward Requiring

Mayor Bowser signed enacted D.C. Act 25-367 "Wage Transparency Omnibus Amendment Act of 2023" which will amend the Wage Transparency Act of 2014. The action puts Washington, D.C. one step closer to joining the growing list of jurisdictions requiring pay ranges in job listings and advertisements. If the Act survives the 30-day Congressional review, the new law, which applies to employers with at least one employee in the District, will also require employers to disclose to prospective employees the existence of healthcare benefits they may receive, prior to the first interview. It will also expand DC's current law to prohibit employers from seeking wage history information of prospective employees or screening prospective employees based on their wage history. The Office of the Attorney General will have enforcement authority. If the Act is not disapproved during the upcoming 30-day Congressional review, it will become effective as of

June 30, 2024.

Required Pay Disclosures in Job Listings and Position Descriptions Advertised
The Act will require that employers provide the minimum and maximum projected salary or hourly pay in all job listings and position descriptions advertised. In stating the minimum and maximum salary or hourly pay for the position, the range must extend from the lowest to the highest salary or hourly pay that the employer in good faith believes at the time of the posting it would pay for the advertised job, promotion, or transfer opportunity.

Healthcare Benefit Disclosure Prior to Interview
The Act also requires that employers include information on the *healthcare* benefits offered to employees before the first interview. The law does not define "first interview," nor does it specify whether a general description of the benefits is sufficient or if more detailed information may be required. There is no requirement, however, to include the healthcare benefit information in the job posting for the open position.

If an employer fails to disclose the pay range in a job listing or advertised position description, or fails to disclose the existence of healthcare benefits prior to the interview, the prospective employee is permitted to ask about such disclosures.

Prohibition on Seeking or Using "Wage History"
The Act will also limit employers' ability to seek or use a prospective employee's wage history in several ways. First, it prohibits employers from screening prospective employees based on their "wage history," including by requiring that the wage history satisfy minimum or maximum criteria or by requiring the prospective employee to disclose their wage history as a condition of being interviewed or continuing to be considered for an offer of employment. Second, the Act will also prohibit employers from seeking the wage history of a prospective employee from a person who previously employed the individual. The term "wage history" is defined as "information related to compensation an employee has received from other or previous employment." Further, the definition of "compensation" is expansive and includes "all forms of monetary and nonmonetary benefits an employer provides or promises to provide an employee in exchange for the employee's services to the employer."

Required Notice of Rights
Covered employers will also have another notice to add to the collection of required federal and state employment posters. This new Act will require employers to post a notice in a conspicuous place in the workplace notifying employees of their rights under the Wage Transparency Act. The notice must be posted in at least one location where employees congregate.

Enforcement and Potential Remedies
The Act will authorize the Attorney General to investigate whether an employer has violated the Act, including examining witnesses under oath, issuing subpoenas, compelling attendance of witnesses and production of documents, and taking depositions and affidavits. It also allows the Attorney General to bring a civil action against an employer for violating the Act for restitution or for injunctive, compensatory, or other authorized relief for an individual or the public at large. If successful, the Attorney General will be entitled to reasonable attorneys' fees and costs and statutory penalties equal to any administrative penalties provided by law.

Next Steps for Employers
While the Act still must pass Congressional review, DC employers should start taking steps now to prepare to comply with these requirements and prohibitions. Employers should consider how they will appropriately identify pay ranges to include in their job postings. For those employers who have already begun to include pay ranges in all of their postings to address the patchwork of laws in other jurisdictions requiring such disclosures, you should consider whether your current approach to disclosures will be compliant in DC.

In addition to preparing to update job postings and advertised job descriptions, employers should also consider training for hiring managers, talent acquisition, and other human resources professionals to ensure there is a process in place to disclose healthcare benefits prior to a first interview and the restrictions on seeking or using wage history. Additionally, employers should also consider conducting a privileged review of employee compensation to determine whether there are unexplained discrepancies that should be addressed prior to publishing pay ranges.
CLICK HERE.

COURT CASES

Magistrate Judge Recommends No FCRA Liability for Accurately Reporting a Publicly Available Conviction that was Expunged

A magistrate judge in the Northern District of Georgia recently recommended granting summary judgment in a Fair Credit Reporting Act (FCRA) case in favor of a background reporting company on the grounds that a report given only to the consumer is not a consumer report and including a valid conviction on a report does not violate the FCRA as long as its expungement is also included.

In *Peeples v. National Data Research, Inc.* (NDR), the plaintiff applied to a pre-med program at a school that required a background report from NDR as part of its application requirements. NDR's report on the plaintiff listed a 2003 criminal conviction for "giving false information." The 2003 conviction, however, was expunged by court order in December 2019. The report from NDR did not contain any information about the expungement and NDR did not have a policy to investigate whether court records have been expunged absent a consumer dispute.

NDR provided the background report to the plaintiff only. The plaintiff then requested removal of the conviction due to the expungement. NDR confirmed the plaintiff was convicted for giving false information and the judgment was expunged. It updated the report to include the expungement but did not remove the underlying conviction.

The plaintiff sued NDR for violation of two sections of the FCRA: § 1681e(b) for failing to follow reasonable procedures to assure maximum possible accuracy in the report; and § 1681i for failing to perform a reasonable reinvestigation and correct or suppress the expunged record and maintain reasonable procedures to prevent that inaccurate information from reappearing.

In the report and recommendation, the magistrate judge began the analysis by noting that the Eleventh Circuit draws a distinction between a consumer report and a credit file. A consumer report requires communication of the information to a third party. Section 1681e(b) relates solely to information in a consumer report. Because NDR provided the report only to the plaintiff, it was not a consumer report. NDR's knowledge the plaintiff would be submitting the report to her school did not make it a consumer report because NDR was not the one providing it to a third party. As a result, the magistrate judge recommended the district court grant NDR summary judgment on the § 1681e(b) claim.

When considering the plaintiff's claim under § 1681i, the court accepted that the report was inaccurate/incomplete when it did not include the expungement information, that the plaintiff notified NDR, and that her dispute was not frivolous, focusing only on whether NDR conducted a reasonable reinvestigation of the disputed item — the conviction — and whether failure to remove it caused the plaintiff harm. The magistrate judge noted that federal courts have generally held that including a valid conviction on a background report does not violate the FCRA, even if that conviction was later set aside, dismissed, or expunged. "For purposes of FCRA reporting, the historical fact of [the plaintiff's] conviction was not altered by the expungement order, and the FCRA expressly permits consumer reporting agencies to report 'records of convictions of crimes.' 15 U.S.C. § 1681c(a)." Federal law, not South Carolina law, dictates the conviction is still a conviction. Ultimately, while the original report of conviction was incomplete, once NDR modified and corrected the report to include the expungement, nothing more was required and summary judgment was recommended in NDR's favor on this claim.
CLICK HERE.

CJEU Rules on Processing of Sensitive Data and Compensation Under the GDPR

On December 21, 2023, the Court of Justice of the European Union ("CJEU") issued its judgment in the case of *Krankenversicherung Nordrhein* (C-667/21) in which it clarified, among other things, the rules for processing special categories of personal data (hereafter "sensitive personal data") under Article 9 of the EU General Data Protection Regulation ("GDPR") and the nature of the compensation owed for damages under Article 82 of the GDPR.

Background
The case related to the processing of an incapacitated employee's personal data, including health data, by the medical service provider ("MDK") of a health insurance fund in Germany. Under applicable law, the MDK draws up reports on the capacity of individuals insured by the health insurance fund to work. These may include reports concerning the health of MDK's own employees. After becoming aware of the fact that a report concerning himself had been prepared, an employee of MDK sought compensation under Article 82 of the GDPR.

The CJEU's Ruling
In its judgment, the CJEU ruled that in order to process sensitive personal data under the GDPR, there must exist both a legal basis under Article 6 of the GDPR and an applicable exception under Article 9 of the GDPR.

The CJEU also held that the rules and limitations on the processing of sensitive personal data under Article 9.2(h) (which allows processing of sensitive personal data where necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services) and Article 9.3 of the GDPR (which provides that processing based on Article 9.2 (h) of the GDPR must be conducted by or under the responsibility of a professional subject to the obligation of professional secrecy) are also applicable to a situation in which a medical service provider processes health data of its employees in its capacity as medical service provider to assess their working capacity. In other words, the medical service provider could rely on Article 9.2 (h) of the GDPR to process its employees' health data. The CJEU also clarified that Article 9.3 of the GDPR does not, by itself, require the controller to establish specific restrictions regarding the ability of work colleagues to access the health data of an employee.

On the interpretation of Article 82 of the GDPR, the CJEU held that the GDPR establishes a system of fault-based liability in which the controller's fault is presumed, unless it is capable of proving that it is not in any way responsible for the event giving rise to the damage. On the nature of the compensation owed to the data subject under Article 82 of the GDPR, the CJEU clarified that it is purely compensatory, and not punitive in nature.
Read the judgement.
CLICK HERE.

Can you revoke an employment offer if the candidate fails a drug test?
The Human Rights Tribunal of Alberta recently determined that an employer did not discriminate against a job candidate by revoking an offer of employment after the job candidate failed a pre-employment drug test.

The candidate was offered a job as Business Continuity and Emergency Management Advisor. The position was classified as safety-sensitive, and the offer of employment specifically required the candidate to take a pre-employment drug test. The candidate testified that:

- he understood the job offer was conditional and that he would have to undergo a pre-employment drug test; and
- the drug testing company informed him that cannabis was one of the substances that he was being tested for.

The drug test came back positive for cannabis. As a result, the employer revoked the job offer.

The candidate alleged that in revoking the job offer, the employer discriminated against him based on a physical disability in contravention of Alberta's human rights legislation. Specifically, he alleged that he suffered from symptoms related to Hashimoto's disease and that he used cannabis for medical purposes. The Tribunal accepted that the candidate suffered from a physical disability.

However, an obstacle for the candidate in this matter was that he only informed the employer of his disability and his medical use of cannabis *after* the job offer was revoked. Therefore, the Tribunal found that the employer could not have had knowledge of the candidate's physical disability at the time it revoked the job offer. Furthermore, there were no indicators of a disability triggering a duty to inquire on the employer's part.

Based on the above, the Tribunal determined that the candidate's disability played no role in the revocation of the job offer and that the employer did not discriminate against the candidate.

Takeaway for Employers
This is a welcome decision for employers with safety-sensitive positions. It supports placing a positive onus on employees to appropriately disclose disability-related issues to their employer.
Each case needs to be reviewed based on its own facts. There may be times when it is in an employee's best interest to voluntarily disclose a disability, and there may be others where indicators exist that trigger an employer's duty to inquire. Employers are well-advised to follow the lead of the employer in this case and ensure that offers of employment

clearly articulate the conditions and expectations related to pre-employment drug and alcohol testing.
We recommend that employers seek legal advice prior to implementing a drug or alcohol testing policy and prior to taking any disciplinary action against an employee who fails a drug or alcohol test.
CLICK HERE.

INTERNATIONAL DEVELOPMENTS

UK-US data bridge: ICO publishes updated TRA guidance

Following the implementation of the UK-US Data Bridge in October 2023, the ICO has updated its Transfer Risk Assessment guidance with a specific section on TRAs relating to transfers to the United States.

The updated guidance makes it clear that can parties rely on the analysis published by Department of Science, Innovation and Technology in relation to the Data Bridge when making data transfers on the basis of an alternative mechanism.

Data Bridge
The UK-US 'Data Bridge' took effect on 12 October 2023. It is an extension of the EU-US Data Privacy Framework, approved by the European Commission as adequate in respect of transfers from the EU to the US. As with previous, similar transatlantic arrangements, it can only be relied upon in respect of transfers to recipients who are certified under the scheme. As we highlighted in our analysis of the Data Bridge, this means that a TRA is still required for transfers to the US based on other transfer mechanisms. However, the DSIT analysis is still relevant in these circumstances. The ICO concludes that "*it is reasonable and proportionate for you to rely on the DSIT analysis in your TRA, regardless of whether the personal information you are transferring is categorised as low, medium or high harm risk*."

ICO guidance on relying on the DSIT analysis
The ICO guidance states that a broad section of the DSIT analysis was directed at the application of relevant of US laws and practices more generally. It considered US respect for the rule of law and fundamental rights and freedoms, the existence of an effective and independent supervisory authority, and its relevant international commitments. The framework for public authorities to access personal data following transfer to the US was considered to be satisfactory and underpinned by appropriate safeguards and redress.

To that end, organisations are encouraged to simply incorporate the DSIT analysis into their TRAs by reference, documenting that:

- the DSIT analysis concludes that US laws and practices provide adequate protections for people whose personal data is transferred to the US;
- it is reasonable and proportionate to rely on the DSIT analysis because the scope of assessment is as required under Article 45 UK GDPR; and
- any published updates will be kept under review.

Helpfully, the ICO provides examples of suitable wording for a TRA using the above direction, which can be found as part of the overall guidance here and helps to significantly streamline the TRA process.
CLICK HERE.

EU Releases Data Act to Facilitate Access and Use of Data

On 22 December 2023, the Regulation on harmonized rules on fair access to and use of data ("Data Act") was published in the EU's Official Journal.

The Data Act lays down rules on fair access to and use of personal and non-personal data across all economic sectors generated by connected products and digital related services.

In a nutshell, the Data Act:

- Lays down rules on B2B and B2C data access. Manufacturers and providers are obliged to design products and services in such a manner that generated data are directly accessible to users, and to provide information to users on generated data, its accessibility, and users' rights. At the users' requests, data holders are required to make the data available to users or to third parties without undue delay, free of charge and, where applicable, continuously and in real time. These obligations apply to connected products and related services placed on the EU market, irrespective of the place of establishment of the manufacturers and providers.
- Establishes a ban on unfair contractual terms on data sharing and introduces non-binding model

contractual terms.

- Provides for a harmonized framework for the access and use of data held by the private sector, by public sector bodies, the Commission, the European Central Bank, and EU bodies.
- Introduces restrictions to non-EU governmental access and international transfers of non-personal data, by requiring providers of data processing services to take technical, organizational and legal measures to prevent unlawful access and transfers.
- Introduces requirements to enable switching between providers of cloud services and of other data processing services, by requiring providers to take all reasonable measures to facilitate the process of achieving functional equivalence in the use of the new service. Costs arising from the switching process can only be charged to the customers until 12 January 2027.
- Introduces interoperability requirements for participants in data spaces that offer data or data services, data processing service providers, and vendors of applications using smart contracts.
- Includes an obligation for EU Member States to lay down rules on penalties for infringements of the Data Act, and EU supervisory authorities may impose administrative fines as provided in the EU GDPR for certain infringements of the Data Act.

The Data Act enters into force on 11 January 2024. Most of its rules will apply from 12 September 2025.
CLICK HERE.

CJEU rules that a credit score constitutes automated decision making under the GDPR

On 7 December 2023, the Court of Justice of the European Union (CJEU) issued a landmark judgment on Article 22 of the General Data Protection Regulation (GDPR), focused on decision making based solely on automated processing that produces legal effects concerning the data subject, or similarly significantly affects the data subject (ADM). The case involved a leading German credit reference agency, Schufa (Case C-634/21). The judgment has significant implications for organisations using any kind of ADM, including scoring systems and systems that use Artificial Intelligence (AI). Allen & Overy previously published an update on the Advocate General's Opinion on the case back in March 2023.
In a further GDPR judgment in relation to Schufa, the CJEU also ruled that they could not lawfully retain information from a public register related to debt, for a time extending beyond the public register's retention period. Please see our blog on this judgment here.

Background to the Schufa ADM judgment
The case emerged under the following circumstances. A loan application was refused based on the data subject's Schufa score, used as a core component in the loan decision. Following a data subject access request (Article 15 GDPR), Schufa provided the data subject with the score and explained, in high level terms, the methods used to calculate that score. However, Schufa cited trade secrecy as justification for not providing information related to the weighting that lay behind the scoring system.

The data subject then took a complaint to the Data Protection and Freedom of Information Commissioner for the Federal State of Hesse, Germany (the HBDI). The HBDI found that there was no established case that Schufa's credit score processing was non-compliant with Section 31 of the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) which governs the requirements of calculating scores. It also confirmed that Schufa does not need to share the details or mathematical formula related to how information about an individual is weighted to create the individual's Schufa score. The data subject appealed the HBDI's decision to the Administrative Court, Wiesbaden, Germany. That court then made a reference to the CJEU.

Reference to the CJEU
The key question of the reference was as follows: "*whether Article 22(1) of the GDPR must be interpreted as meaning that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes 'automated individual decision-making' within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person.*"

The pivotal issue in the case focused on Article 22 GDPR and whether the Schufa score constituted a decision solely based on automated decision making and whether that decision produced legal effects concerning the data subject or it

similarly significantly affects them and thus whether Schufa should have shared more details on the logic behind the decision.

Under Article 22 GDPR, the data subject has the right not be subject to such ADM. There are exceptions under Article 22(2), specifically: (a) the decision is necessary for the performance of contract between the data subject and a data controller; (b) the decision is authorised by Union or Member State law to which the controller is subject and there are safeguards to protect the data subject; and (c) the decision is based on the data subject's explicit consent. If relying on Article 22(2)(a) or (c) controllers will have to offer human intervention and a way for the data subject to express a view or contest the decision.

The key elements of the ruling

The CJEU found:

1. The broad scope of the concept of 'decision' is confirmed by Recital 71 GDPR. That concept is broad enough to encompass calculating a credit score based on a probability value.
2. A credit score based on probability value in this context affects, at the very least, the data subject significantly.
3. By calculating a credit score, a credit reference agency makes an automated decision within the terms of Article 22 GDPR when a third party draws strongly on the probability value or score to establish, implement or terminate a contractual relationship with the data subject. The CJEU noted a risk of circumventing Article 22 of the GDPR and a lacuna in protections if a narrow approach was taken and the Schufa score was only regarded as preparatory.
4. That Article 22(1) GDPR provides for a prohibition in principle, i.e. the infringement doesn't need to be invoked individually by a data subject making a request.
5. The question of whether Section 31 BDSG constitutes a legal basis in conformity with EU law will now have to be examined by the referring Administrative Court of Wiesbaden.

Wider implications

The judgment is part of a trend towards broad and data subject weighted interpretations of the GDPR by the CJEU, turning it into consumer rather than privacy law. The CJEU's judgment on Article 22 GDPR was set out in broad terms and can be applied to other situations related to scoring systems. The judgment refers to a contractual relationship with the data subject in general terms rather than just the specifics of loan agreement process, indicating the potential breadth of relevance.

The judgment could therefore have implications for a range of scoring processes and decision making; for example, credit reference agencies also provide services for employment checks and anti-money laundering services (AML) can also offer digital services based on scores.

Although the judgment has broad implications, it does not follow that a large number of automated scoring systems are immediately caught by Article 22 GDPR, or are immediately unlawful. It will depend on how the score relates to the final decision made and what role it plays as a factor under consideration. The controller may also have a legal basis to carry out that ADM and safeguards in place as specified under Article 22 GDPR. There is now a significant expectation that data protection authorities need to provide guidance on what "draws strongly" means in practice.

What comes next from data protection authorities?

A number of German Data Protection Authorities (DPAs) have issued statements following the judgment. The Hamburg DPA issued a statement, hailing the "*ground-breaking importance for AI-based decisions*" and also noting that it has "*has consequences far beyond the scope of credit agencies – because it is transferable to the use of many AI systems*". The DPA also gave an example of AI analysing which patients are particularly suitable for a medical study, as an illustration of where the judgment may also make a difference.

The Data Protection Authority for Lower Saxony has also issued a statement and indicated: "*The CJEU's view on the interpretation of the term 'automated decision' could also have further implications, for example on systems that prepare decisions with the help of algorithms or artificial intelligence or make them 'almost alone', so to speak*".
Given the hype around, and importance of, AI, particularly generative AI, we can therefore expect further decisions and guidance from DPAs in 2024, setting out how the judgment will apply in a range of scenarios.

The European Data Protection Board (EDPB) may also need to update its guidelines on automated decision making and profiling. The guidelines were adopted in 2018 and will soon be six years old. While the Schufa CJEU judgment does not contradict the EDPB's guidance, for example the EDPB had already found that Article 22 operated as prohibition in principle, the EDPB may want to expand on the wider implications and explain in more detail what the judgment means in practice, including the concept of "draws strongly" in decision making.

Controllers will need to work through the following steps:

1. Identify any processes and systems using Schufa scores or any other scores or probability values, including when deploying AI systems.
2. Assess whether these systems, including when contracted to third parties, make any decisions that "draw strongly" from the score and would thus now be caught by Article 22(1 If so, can adjustments be made to ensure that reliance on the score in the final decision falls below the "draws strongly" test?If the answer remains that Article 22(1) applies, the controller will need to find a specific legal basis under Article 22(2) to carry out the ADM and apply Article 22(3) safeguards. If the controller is using special category data, the further conditions of Article 22(4) apply.
3. It may currently be the case that certain organisations do not have a contract in place and have not obtained explicit consent as a relevant legal basis. Some EU Member States could seek to provide new national legislation as a legal basis alongside appropriate safeguards.
4. If Article 22(1) applies, the controller will need to meet the transparency requirements of Articles 13 or 14 and 15 GDPR. The controller may need to update existing privacy notices and information pop-up windows. The information must include, at least, meaningful information about the logic involved, as well as the significance and the envisaged consequences of the processing for the data subject.
5. The guidance provided by the UK data protection regulator, the Information Commissioner's Office (ICO), on explainabilty and AI can likely be helpful in this situation.
6. Contracts may also need to be re-examined in a number of different contexts – both the contract between the data subject and the organisation making the final decision, and the contract between the two organisations.
7. Following the judgment, the controller may need to review its data protections impact assessments and other documentation such as legitimate interest assessments and records of processing activities.

Schufa has issued a press release about the judgment. It welcomes the clarification that the judgment provides and notes that: "*The overwhelming feedback from our customers is that payment forecasts in the form of the SCHUFA score are important for them, but are usually not the only decisive factor for concluding a contract*". This indicates that "draws strongly" test will be a key consideration for companies.

Litigation risk

Lastly, in light of the EU Representative Actions Directive (2018/1828) and the increasing trend for data litigation, there is a risk that compensation claims may be launched not just against Schufa but also against organisations using the Schufa score. Allen & Overy's blog from May 2023 assesses the recent CJEU jurisprudence on compensation, including the finding that mere infringement of the GDPR does not confer a right to compensation. Allen & Overy's blog on the collective redress action for consumers in Germany from March 2023 considers the incoming implementation of the EU Representative actions under the Directive (EU) 2020/1828. A key question will be whether a de minimis threshold of equal damage across a class action claim is likely in Article 22 GDPR cases.

Looking ahead

As we look ahead to 2024 we can expect the Schufa judgment to play an important role in how AI is used in automated decision making and where the boundary falls between automated and partially automated decisions. Companies should look out for new guidance and enforcement decisions from DPAs in the year ahead.
CLICK HERE.

Transfers of personal data outside the European Union: the French Data Protection Authority (CNIL) publishes a draft practical guide to carry out a Transfer Impact Assessment

The draft guide is published in the context of a public consultation. Organisations have 1 month to submit their observations

to the CNIL. This article walks you through the context in which CNIL publishes this guide, its content and the keys takeaways.

Why the CNIL publishes this practical guide?
The General Data Protection Regulation ("GDPR") aims at ensuring an equivalent level of protection to personal data within the European Union ("EU") by imposing a regulatory framework which applies to all processing carried out within the EU or relating to individuals residing in the EU.

Some companies may transfer personal data outside the EU as part of their activities, for example by using service providers located in third countries, by using cloud services, or by communicating personal data to a parent company or subsidiaries. This raises the question of the protection of personal data transferred outside the EU, to countries that do not have the same legislation as the EU.

Under the GDPR, personal data must be offered the same level of protection afforded by the GDPR within the EU. This is the case, for example, when personal data is transferred to a country benefiting from an adequacy decision, i.e. a country recognised by the European Commission as offering an adequate level of protection that does not require the implementation of additional measures.

In the absence of an adequacy decision, the data exporter, whether acting as a controller or a processor, must implement measures to compensate for the lack of data protection in the third country, receiving personal data, by providing appropriate safeguards (Binding Corporate Rules (BCR), Standard Contractual Clauses (SCCs), etc.).

In its "Schrems II" judgment of 16 July 2020, the Court of Justice of the European Union (CJEU) ruled that standard contractual clauses were insufficient to ensure an effective protection of personal data, as they do not bind third countries due to their contractual nature.

As a consequence, the CJEU ruled that the data exporter must (i) verify whether the legislation of the third country receiving the personal data offers a level of protection that is essentially equivalent to that guaranteed in the EU and (ii) determine the appropriate additional measures where necessary, in addition to implementing the appropriate safeguards.
In order to fulfil this obligation, and where the transfer of personal data is based on a transfer tool listed under Article 46 of the GDPR, the data exporter, in collaboration with the data importer, must carry out a data transfer impact assessment (also referred to as a "TIA").

The European Data Protection Board (EDPB) has already published, in June 2021, its recommendations on measures to supplement transfer tools to ensure compliance with the EU level of personal data protection in which the EDPB details the different steps to be followed by the data exporter when carrying out a TIA and provides information on the supplementary measures that can be implemented and their effectiveness.

Up until now, organisations have essentially relied on these recommendations and on the recommendations 02/2020 on essential European safeguards for surveillance measures to carry out TIAs.

It is in this context that the CNIL decided to draft its own practical guide to, in its own words, "*help data exporters carry out their TIAs*".

At this stage, the CNIL is publishing a draft guide for public consultation until February 12, 2024. Publication of the definitive guide is scheduled for 2024.

What this guide contains?
This guide should be used as a methodology available for data exporters and enabling them to carry out a TIA.
It should be noted that the CNIL has very much relied on the EDPB recommendations when elaborating this guide. Nevertheless, this guide is intended to be more practical than the EDPB recommendations, since it includes a TIA template that can be used as is by data exporters. This TIA template takes indeed the form of a table to be completed, including boxes to be ticked, which includes and reorganises the different steps and elements mentioned by the EDPB in its recommendations. The guide includes a first part dedicated to the questions to be asked in order to determine whether a TIA is necessary:

- *Is the data in question personal data?*

- *Is there a transfer of personal data?*
- *What is the qualification of the actors implicated?*
- *Does the transfer comply with all the principles of the GDPR and, in particular, can you minimise the amount of personal data transferred or transfer anonymised data rather than personal data?*
- *Can your data be transferred to a country that has been recognised by the European Commission as offering an adequate level of protection?*

The guide then provides a TIA template based on the six steps mentioned by the EDPB for carrying out a TIA, which are as follows:

1. *Know your transfer*
2. *Document the transfer tool used*
3. *Evaluate the legislation and practices in the country of destination of the data and the effectiveness of the transfer tool*
4. *Identify and adopt supplementary measures*
5. *Implement the supplementary measures and the necessary procedural steps*
6. *Re-evaluate at appropriate interval the level of data protection and monitor potential developments that may affect it.*

The compilation of the different steps and information provided by the EDPB in its recommendations, in the form of a table listing all the elements that must be included in a TIA, appear to be useful and practical for data exporters.

What are the key takeaways of this guide?
Some elements are worth noting:

- This guide does not constitute or contain, and is not intended to contain, an assessment of the legislation and practices of third countries. The CNIL therefore does not take a position on the level of personal data protection afforded by countries outside the EU, leaving it up to organisations to assess the legislation and practices of third countries.
- The template includes a section dedicated to the transfer tools used, which corresponds to step 2 of the TIA, also listed by the EDPB. As provided by both the EDPB and the CNIL, a TIA is not required when the recipient country benefits from an adequacy decision. However, with this template, which is a TIA template, it seems that the data exporter should complete step 1 (know your transfer) and step 2 (document the transfer tool used), for all transfers carried out, regardless of the transfer tool. In this context, the CNIL's requirements seem to go beyond the EDPB's requirements. If this draft guide is adopted as is, organisations that do not carry out TIAs for transfers to countries benefiting from an adequacy decision, and rightly so, will have to review their compliance strategy if they wish to align themselves with the CNIL's more stringent requirements.
- If onward transfers are carried out by the data importer, the CNIL considers that a specific TIA should be carried out for each type of onward transfer. The EDPB recommendations are not that precise on this particular topic, since the EDPB merely states that "*When mapping transfers, do not forget to also take into account onward transfers*". Covering the initial transfer and onward transfers within the same TIA does not therefore seem to be the CNIL's recommendation. Another document will have to be prepared for each onward transfer, which increases the burden imposed on the data exporter, as described in the EDPB recommendations.
- The CNIL also increases the role and obligations of the data importer, particularly when it is acting as a processor. In its Schrems II judgment, the CJEU ruled that "*controller or processor [must] verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law [...]*". The data importer may be a data controller or a data processor. The CNIL is rigorous towards the data importer since the CNIL indicates that the importer's cooperation is essential for the TIA to be carried out.

The CNIL has a much stricter interpretation of this duty to cooperate when the data importer is acting as a processor. The CNIL states that "*In the context of a relationship between a controller and a processor, the transmission of this information to the controller by the processor is part of the latter's obligations under Article 28 of the GDPR, and in particular Article 28(3)(h)"*. The CNIL also considers that "*the transmission by the importing processor of a simple conclusion or an executive summary of its assessment, without the provision of concrete information on the legislation of the third country and the*

practices of the authorities, as well as on the circumstances of the transfer, does not enable the processor to fulfil its obligations under Article 28 of the RGPD". This rigorous interpretation of Article 28 of the GDPR requires the data processor importer to be significantly involved as it must provide concrete information on the legislation of the third country and the practices of its authorities.

This practical guide, which is still awaiting its final publication in 2024, is not mandatory but constitutes a tool helping organisations to comply with TIA requirements. The CNIL's draft practical guide is available in French and in English. Organisations have until February 12, 2024 to submit their comments.
CLICK HERE.

Can you revoke an employment offer if the candidate fails a drug test (Alberta, Canada)?

The Human Rights Tribunal of Alberta recently determined that an employer did not discriminate against a job candidate by revoking an offer of employment after the job candidate failed a pre-employment drug test.
The candidate was offered a job as Business Continuity and Emergency Management Advisor. The position was classified as safety-sensitive, and the offer of employment specifically required the candidate to take a pre-employment drug test. The candidate testified that:

- he understood the job offer was conditional and that he would have to undergo a pre-employment drug test; and
- the drug testing company informed him that cannabis was one of the substances that he was being tested for.

The drug test came back positive for cannabis. As a result, the employer revoked the job offer.

The candidate alleged that in revoking the job offer, the employer discriminated against him based on a physical disability in contravention of Alberta's human rights legislation. Specifically, he alleged that he suffered from symptoms related to Hashimoto's disease and that he used cannabis for medical purposes. The Tribunal accepted that the candidate suffered from a physical disability.

However, an obstacle for the candidate in this matter was that he only informed the employer of his disability and his medical use of cannabis *after* the job offer was revoked. Therefore, the Tribunal found that the employer could not have had knowledge of the candidate's physical disability at the time it revoked the job offer. Furthermore, there were no indicators of a disability triggering a duty to inquire on the employer's part.

Based on the above, the Tribunal determined that the candidate's disability played no role in the revocation of the job offer and that the employer did not discriminate against the candidate.

Takeaway for Employers
This is a welcome decision for employers with safety-sensitive positions. It supports placing a positive onus on employees to appropriately disclose disability-related issues to their employer.

Each case needs to be reviewed based on its own facts. There may be times when it is in an employee's best interest to voluntarily disclose a disability, and there may be others where indicators exist that trigger an employer's duty to inquire. Employers are well-advised to follow the lead of the employer in this case and ensure that offers of employment clearly articulate the conditions and expectations related to pre-employment drug and alcohol testing.
CLICK HERE.

Argentina: New adequacy decision obtained from the European Union for the international transfer of personal data

The European Commission ("**Commission**") concluded that personal data transferred from the European Union (EU) to Argentina are adequately protected and, therefore, can continue to flow freely from the EU to Argentina.

In more detail
On 15 January 2024, the Commission published its conclusions regarding the first review of the adequacy decisions adopted

— pursuant to Article 25(6) of Directive 95/46/EC ("**Directive**") — in 1995. In these decisions, the Commission had determined that 11 countries or territories, including Argentina, guaranteed an adequate level of protection of personal data. This allowed data transfers from the EU to these countries.

With the entry into force of the EU General Data Protection Regulation 2016/67914 in 2018, it was established that adequacy decisions issued under the Directive would remain in force but be subject to review every four years.

In this first review, the Commission determined that data protection frameworks in the countries and territories under review have evolved through legislative reforms and regulations of the data protection authorities, among others.

In the case of Argentina, the Commission highlighted the importance of the independence of the Agency for Access to Public Information as a supervisory authority and the ratification of Convention 108+ in 2023. In addition, the Commission noted that the Data Protection Bill introduced in Congress could consolidate these developments, further strengthening the data protection framework in the country.

This decision is relevant as it positions the country at the forefront in the protection of personal data and enables fluidity and security in international operations.
CLICK HERE.

Quebec Law No. 25: a Little-known Privacy Law with a Big Reach

In late 2021, the Quebec legislature passed "The Privacy Legislation Modernization Act" or Law No. 25 ("**Law 25**"), which was designed to modernize and make significant changes to Quebec's existing privacy framework. Previously, Quebec's privacy regime was very industry-specific, but Law 25 is far broader and has general application. It grants significant new privacy rights for residents of Quebec and establishes heightened obligations for in-scope public and private organizations.

Of particular note for businesses outside Quebec, Law 25 applies to all organizations "carrying on an enterprise" in Quebec that collect, process, use, or disclose Personal Information of individuals located in Quebec. An "enterprise" is defined as carrying on an "organized economic activity," but that activity does not have to be commercial in nature. Entities deemed "enterprises" under Law 25 include unions and medical practices, whereas spiritual and religious organizations are not considered enterprises, as their main purpose is not "economic." Learning From a Decade of Experience: Quebec's Private Sector Privacy Act, at 1.2.3 and 1.2.4. This means that the law likely applies to both for-profit and nonprofit organizations located abroad that process Personal Information of Quebec residents. There also are no minimum thresholds in terms of number of Quebec residents' Personal Information processed or revenue generated nor broad-brush exemptions under Law 25 for categories of data or entities that are already regulated under different regimes. In short, Law 25 likely is in scope for any organization, either within or outside the borders of Quebec, which processes Personal Information associated with one or more of Quebec's approximately 9 million residents.

Law 25 does not adopt the familiar terminology of "controller" or "processor." However, Law 25 does stipulate that processing of Personal Information by third persons on behalf of an in-scope organization requires a written contract "to protect the confidentiality of the Personal Information communicated, to ensure that the information is used only for carrying out the mandate or performing the contract, and to ensure that the mandatary or person does not keep the information after the expiry of the mandate or contract." *Law 25* at Section III, para. 18.3.

Law 25 will be enforced by the Commission on Access to Information ("**CAI**"), and fines range up to 2% - 4% of worldwide turnover (revenue) or $10 - $25 million CAD, depending on the severity of the violation. *Id.* at Section VII, paras. 90.12-91. Finally, Law 25 gives rise to a new private right of action, allowing individuals to bring claims against in-scope organizations for recovery of statutory damages. *Id.* Law 25 also allows harmed employees to bring collective actions.

Given the above, Law 25 is comparable to the General Data Protection Regulation ("GDPR") and has a broader reach than any U.S. state omnibus privacy law. When compared to Canada's federal law, the Personal Information Protection and Electronic Documents Act ("PIPEDA"), Law 25 has more onerous requirements and poses a greater potential for liability. For example, PIPEDA does not afford residents expansive data subject rights, whereas Law 25 does offer

Quebec residents with a full set of individual rights. Law 25 also has stricter consent requirements than PIPEDA.

Law 25's requirements and staggered compliance timeline
Law 25's requirements become effective in phases. Below is a list of Law 25's primary requirements and mandatory compliance dates:

September 22, 2022

1. **Data Protection Officer ("Privacy Officer") Appointment** – In-scope organizations must appoint a Privacy Officer to oversee the data subject requests, data breach reporting, and Privacy Impact Assessment processes. The Privacy Officer need not be located in Quebec and the role can be delegated to the highest senior employee responsible for overseeing compliance. In-scope organizations must publish the name, title, and contact information for the Privacy Officer on their websites. *Id.* at Section I, para. 3.1.
2. **Breach Reporting** – In-scope organizations must notify the CAI and impacted individuals as soon as possible after discovery of a data breach that poses a "high risk of serious injury." In-scope organizations must also maintain an internal register of all qualifying data breaches, which may be requested by the CAI. *Id.* at Section I, para. 3.5.
3. **Disclosure of Biometric Use** – In-scope organizations must disclose whether they intend to collect and/or use any biometric data within a service, product, or system to the CAI sixty (60) days prior to implementation. *Id.* at Section III.

September 22, 2023

1. **Privacy Policy** – In-scope organizations must publish a privacy policy on their websites. *Id.* at Section II, para. 8.
2. **Privacy Impact Assessments ("PIA(s)")** – In-scope organizations must conduct a PIA when certain triggering circumstances occur, such as when Personal Information is being transferred outside of Quebec or when risky processing occurs, including the processing of Sensitive Personal Information. The PIA requirement also applies where an in-scope organization entrusts a service provider, processor, or another third party outside Quebec with the task of collecting, using, communicating, or keeping Personal Information on their behalf. *Id.* at Section I, para. 3.3.
3. **Transparency & Consent** – In-scope organizations must regularly audit their processes for collecting, storing, processing, and sharing Personal Information to ensure they are in compliance with Law 25's requirements. Further, in-scope organizations must obtain explicit opt-in consent prior to collecting, storing, processing, and sharing Personal Information, subject to certain exceptions. *Id.* at Section II, para. 12. Law 25 also requires in-scope organizations to take an opt-in approach with respect to cookies and other tracking technologies, meaning that certain cookies cannot deploy on an in-scope organization's website without the user's affirmative consent to the deployment of such cookies. *Id.* at Section II, paras. 8.1 and 9.1. Law 25 does not specify the types of cookies that will require opt-in consent but rather states that the cookies and similar tracking mechanisms whose function allows a user to be "identified, located, or profiled" be subject to the opt-in requirement. Without further guidance from the CAI on this subject, in-scope organizations should consider obtaining opt-in consent for the deployment of all non-essential cookies.
4. **Data Minimization** – In-scope organizations must ensure Personal Information is destroyed and/or anonymized when retention is no longer reasonably necessary. *Id.* at Section 3, para. 23.
5. **Data Subject Rights** – In-scope organizations are required to permit individuals to submit, and must respond to, certain privacy rights requests, such as the right to be informed, access, rectification, withdrawal of consent, and restriction of processing. *Id.* at Section I, para. 8.

September 22, 2024

1. **Right to Portability** – In-scope organizations must be able to produce a portable record of Personal Information stored about an individual upon request by the individual. *Id.*
2. With the majority of Law 25's requirements currently in effect, and the law becoming fully effective by the end of 2024, we can expect aggressive enforcement by the CAI.

Considerations for in-scope organizations
While Law 25 went into force without much fanfare, organizations should waste no time in considering Law 25's

applicability. The following measures should be considered when assessing the applicability of Law 25 to business operations and preparing to comply:

1. Understand whether Personal Information belonging to a Quebec resident has been or will be collected or processed through any offered service, product, or system;
2. Ensure that when Personal Information is transferred outside of Quebec, a PIA is conducted;
3. Ensure privacy notices are updated to accurately describe Personal Information collection, processing, and use;
4. Determine whether appointing a Privacy Officer is necessary, if one is not already appointed in Canada and/or Quebec;
5. Ensure that certain cookies or other similar tracking technologies are deployed on a website only upon affirmative opt-in by a user; and
6. Develop a clear and actionable strategy for obtaining consent for processing Personal Information of Quebec residents or assess whether a consent exception can be relied upon.

CLICK HERE.

European Commission Approves of Canada's Data Protection Regime (Again)

On January 15, 2024, the European Commission ("**Commission**") renewed Canada's adequacy status under the General Data Protection Regulation ("**GDPR**").[1] You can read the Commission's full report setting out its adequacy decision here (the "**Report**").

The following bulletin will give you a brief overview of the GDPR, the importance of obtaining adequacy status, and why Canada's adequacy status is important for Canadian businesses.

What is the GDPR?

The European Union ("**EU**") enacted the GDPR in May 2018.[2] The GDPR strengthens the protection of all EU citizens with respect to the transfer of their personal data and harmonizes national data privacy laws throughout the EU.[3] The GDPR requires all companies processing the personal data of EU residents, including companies established outside the EU if they operate in the EU, to comply with the data protection rules set out therein.[4] For example, the GDPR requires that companies obtain "specific, informed and unambiguous consent" in order to process an individual's personal data.[5]

What is adequacy status?

Pursuant to the GDPR, if the Commission finds that a country outside of the EU offers an adequate level of data protection, that country can obtain adequacy status.[6] Obtaining adequacy status involves a proposal from the European Commission, an opinion of the European Data Protection Board, an approval from representatives of EU countries, and the adoption of the decision by the European Commission.[7] However, adequacy status may be revoked at any time if the European Parliament and the Council request that the European Commission withdraw, maintain or amend its adequacy decision.[8]
Prior to the GDPR, 11 countries were granted adequacy status under the then *Data Protection Directive* 95/46/EC, namely: Andorra, Argentina, Canada, Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. These adequacy decisions have remained in force so far, even after the GDPR came into effect.

On January 15, 2024, following its review of the 11 existing adequacy decisions, the Commission renewed Canada's adequacy status alongside the other 10 countries with existing adequacy status.[9] The Report concluded that the aforementioned countries' existing data protection frameworks are aligned with the EU's framework and provide significant data safeguards for personal data.[10]
The Commission found that Canada continues to provide an adequate level of protection for personal data transferred from the EU to recipients subject to Canada's federal private sector privacy law, the *Personal Information Protection Electronic Documents Act*[11] ("**PIPEDA**").

What does this mean for Canadian businesses?

If a country has adequacy status, personal data can flow from the EU to that country without the need for any additional data protection safeguards, such as standard contractual rules, the need for additional data processing addenda or authorizations to transfer the data. The additional safeguard requirements could be cumbersome and onerous for some organizations. Canada's adequacy status results in increased efficiency for Canadian businesses transferring personal data from the EU to Canada.

What's next?

To ensure Canada continues to maintain its adequacy status under the GDPR, the federal government will need to bring its privacy laws into closer alignment with the GDPR.

Canada's federal privacy legislation, PIPEDA, is expected to see an overhaul soon. Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts known as the Digital Charter Implementation Act, 2022* ("**Bill C-27**") has completed its second reading in Parliament and is undergoing consideration by the Standing Committee on Industry and Technology.

Bill C-27 introduced bold new measures that will bring Canadian privacy law into closer alignment with the GDPR. Closer alignment with the GDPR will continue to assist Canada in maintaining its adequacy status under the GDPR, allowing Canadian businesses to transfer personal information from the EU to Canada without additional data protection safeguards as discussed above.
CLICK HERE.

Ontario, Canada Human Rights Commission Publishes Policy on Caste-based Discrimination

The Ontario Human Rights Commission recently published a policy statement (Policy) pertaining to "caste-based discrimination" under Ontario's *Human Rights Code*. The Policy advises organizations that they have a legal obligation under the Code to ensure that "their environments are free from discrimination and harassment, bullying or a poisoned environment based on caste and the related grounds"; to investigate claims of caste-based discrimination; and to remedy situations when such discrimination is found.
CLICK HERE.

MISCELLEANOUS DEVELOPMENTS

Rite Aid Settles FTC Allegations Regarding Use of Facial Recognition Technology

On December 19, 2023, the Federal Trade Commission ("FTC") announced that it reached a settlement with Rite Aid Corporation and Rite Aid Headquarters Corporation (collectively, "Rite Aid") to resolve allegations that the companies violated Section 5 of the FTC Act (as well as a prior settlement with the agency) by failing to implement reasonable procedures to prevent harm to consumers while using facial recognition technology. As part of the settlement, Rite Aid agreed to cease using "Facial Recognition or Analysis Systems" (defined below) for five years and establish a monitoring program to address certain risks if it seeks to use such systems for certain purposes in the future.

According to the FTC's complaint, Rite Aid "used facial recognition technology in hundreds of its retail pharmacy locations to identify patrons that it had previously deemed likely to engage in shoplifting or other criminal behavior." The FTC claimed that the technology sent alerts to Rite Aid's employees when patrons were matched with entries in the company's "watchlist database." Rite Aid employees allegedly took action against patrons who triggered the matches by, for example, subjecting them to in-person surveillance. The FTC claimed that Rite Aid failed to consider or address foreseeable harm to patrons by such conduct, including failing to (1) test the technology's accuracy, (2) enforce image quality standards necessary for the technology to function accurately, (3) take reasonable steps to train employees, and (4) "take steps to assess or address risks that its . . . [the] technology would disproportionately harm consumers because of their race, gender, or other demographic characteristics."

The proposed consent order places a number of restrictions and obligations on Rite Aid, including with respect to its use of a "Facial Recognition or Analysis System," which it defines as "an Automated Biometric Security or Surveillance System that analyzes or uses depictions or images, descriptions, recordings, copies, measurements, or geometry of or related to an individual's face to generate an Output." An "Automated Biometric Security or Surveillance System," in turn, is defined as "any machine-based system, including any computer software, application, or algorithm, that analyzes or uses Biometric Information of, from, or about individual consumers to generate an Output that relates to those consumers, notwithstanding any assistance by a human being in such analysis or use, and that is used in whole or in part for a Security or Surveillance Purpose," subject to a few exceptions.

Among other restrictions, the proposed consent order requires that Rite Aid:

- not deploy or use any Facial Recognition or Analysis System for five years, either in a retail store or an online retail platform;
- delete all photos and videos of consumers used in a Facial Recognition or Analysis System, including any data, models, or algorithms derived from such information;
- prior to deploying an Automated Biometric Security or Surveillance System in the future:
- Establish and maintain a monitoring program, that among things, identifies and addresses risks that "will result, in whole or in part, in physical, financial, or reputational harm to consumers" and "any such harms [that] will disproportionately affect consumers based on race, ethnicity, gender, sex, age, or disability, alone or in combination;
    - Develop mandatory notice and complaint procedures that include providing written notice to consumers whose biometric information will be enrolled in the system;
    - Develop a written retention schedule that, among other things, sets a time frame of deletion for biometric information that is no greater than five years, subject to certain exceptions; and
- implement a comprehensive information security program that includes safeguards based on the "volume and sensitivity" of the information that is at risk and the likelihood that the risk could result in unauthorized collection or misuse.

The proposed FTC consent order is subject to a 30-day public comment period following publication in the Federal Register. Rite Aid filed for relief under Chapter 11 of the Bankruptcy Code on October 15, 2023. Accordingly, the settlement is also subject to approval by the U.S. Bankruptcy Court overseeing the company's bankruptcy proceeding.
This settlement was described by the FTC as the first enforcement action by the agency that addresses alleged discrimination through the use of automated decision-making technologies.
CLICK HERE.

New Year - New Statute of Limitations for Complaints filed with the New York State Division of Human Rights

New York has extended the statute of limitations for administrative complaints under the New York State Human Rights Law. On November 17, 2023, Governor Kathy Hochul signed into law Senate Bill S.3255, which amended Section 297-5 of the New York Executive Law. This amendment extends, from one year to three years, the time in which a person may file a complaint of unlawful discrimination with the New York State Division of Human Rights. The Division is the administrative agency that investigates and enforces New York State's Human Rights Law.

Before this amendment, the NYS Human Rights Law contained a one-year statute of limitations for all administrative claims of discrimination other than sexual harassment. The statute of limitations for administrative claims of sexual harassment was three years. Under the new amendment, effective February 15, 2024, the statute of limitations for all administrative claims that arise on or after that date will be three years. Such claims include discrimination on the basis of race, color, creed, national origin, citizenship or immigration status, age, sexual orientation, disability, miliary status, and other protected classes, as well as claims of unlawful retaliation under the NYS Human Rights Law.

The statute of limitations for filing a claim in court under the NYS Human Rights Law is already three years. The amendment provides that administrative claims filed with the NYS Division of Human Rights will now have the same three-year time limit from the date of the alleged unlawful practice.
CLICK HERE.

What is a Negligent Hiring Claim in New Jersey?

Employers' employees often encounter other members of the public. Those interactions can lead to litigation. For example, as addressed in one of my prior blog posts, an employee could be accused of sexually harassing a customer, vendor, or other third party. As discussed in that prior blog post, that could result in potential liability against the employer based upon New Jersey's Law Against Discrimination.

Likewise, an employer who hires an employee with a history of drunk driving offenses could be sued for negligence in hiring if that employee injures a third party while operating a company vehicle intoxicated during company time. In other words, "negligence in hiring" claims are not limited to discrimination claims. The "negligence in hiring" claim may be asserted in addition to a respondeat superior claim (a legal theory in which an employer is responsible for the negligence or wrongdoing of its employees).

Because employers are responsible for "exercising a duty of reasonable care in the selection or retention of its employee," under certain circumstances, an employer can be sued for negligence associated with the hiring of the employee. See, Di Cosala v. Kay, 91 N.J. 159, 170-171 (1982). The negligence in hiring claim has two elements that must be proven by the Plaintiff by a preponderance of the evidence:

1. That the employer "knew or had reason to know of the particular unfitness, incompetence, or dangerous attributes of the employee and could reasonably have foreseen that such qualities create a risk of harm to other persons; and
2. That, thought the negligence of the employer in hiring the employee, the latter's incompetence, unfitness, or dangerous characteristics proximately caused the injury."

Di Cosala v. Kay, 91 N.J. at 173.
Employers should take the following steps to try to limit the liability of this claim. First, employers should conduct reasonable due diligence before hiring an employee. If prior employers will speak with you, I recommend asking about potential prior problems with the prospective employee. Conduct online research to see if there are lawsuits or other claims against the prospective employee. Run background checks to see if the prospective employee has any licensing or other issues. Ask the prospective employee to provide a driver's abstract and for information identifying potential "red flags."

In doing so, please ensure your company files your particular state laws regarding questions and background information you may obtain/ask about. For example, the New Jersey Opportunity to Compete Act, N.J.S.A. 34:6B-11, et. seq., prohibits, amongst other things, a job applicant to fill out a job application or other screening form which asks about their criminal record.
CLICK HERE.

Canada's federal, provincial and territorial privacy authorities have co-published a document entitled Principles for responsible, trustworthy and privacy-protective generative AI technologies (the "**Principles**"), offering critical guidance for organizations that develop, provide and use generative artificial intelligence ("**GenAI**") systems.

GenAI, a subset of machine learning, has gained popularity for its ability to generate diverse outputs such as text, images and audio in response to users' prompts. However, its reliance on vast training datasets and user inputs, often including personal information, poses unique privacy challenges.

The Principles are drafted to apply to organizations that are subject to Canada's public, private and health sector privacy laws. Though the considerations outlined in the Principles are framed as recommendations, many will be mandatory for organizations to comply with applicable privacy legislation.

This bulletin includes a high-level summary of those Principles that apply equally to organizations that develop, provide and use GenAI systems. However, organizations are advised to consult the Principles in full, as they contain additional recommendations, including some that may apply exclusively to developers, providers and/or users of GenAI systems.

Key Principles and Recommendations

According to Canada's privacy regulators, ten key privacy principles that apply to the development, provision and use of GenAI systems are as follows:

1. **Legal Authority and Consent:**
   An organization must have and document its legal authority for collecting, using, disclosing and deleting personal information in the course of training, developing, deploying, operating or decommissioning a GenAI system. Notably, the Principles assert that using GenAI to infer information about an identifiable individual constitutes a "collection" of personal information and therefore requires a valid legal authority, such as consent. When relying on consent as its legal authority, an organization must ensure that such consent is specific, "valid and meaningful", and not obtained through deceptive design patterns. An organization that sources personal information from a third party in connection with a GenAI system must ensure that the third party has collected the personal information lawfully and has a legal authority to disclose the personal information.
2. **Appropriate Purposes:**
   An organization must avoid any collection, use and disclosure of personal information for inappropriate purposes and consider whether the use of a GenAI system is appropriate for a specific application. This includes avoiding the development, putting into service, or use of a GenAI system that violates the "No-Go Zones" already identified by Canadian privacy regulators (such as for discriminatory profiling or generating content that otherwise infringes on fundamental rights), as well as potential emerging No-Go Zones identified in the Principles (such as the creation of content for malicious purposes, e.g., deep fakes).
3. **Necessity and Proportionality:**
   An organization must establish the necessity and proportionality of using GenAI, and personal information within a GenAI system, to achieve the intended purpose(s). The Principles further advocate for the use of anonymized, synthetic or de-identified data, rather than personal information, in GenAI systems whenever possible.
4. **Openness and Transparency:**
   An organization must be transparent about its collection, use and disclosure of personal information, as well as potential risks to individuals' privacy, throughout the development, training and operation of a GenAI system for which the organization is responsible. This includes, for example, clearly stating the appropriate purpose(s) for such collection, use and disclosure of personal information and meaningfully identifying when system outputs that could have a significant impact on an individual or group are created by a GenAI tool. This information should be made readily available before, during and after use of the GenAI system.
5. **Accountability:**
   A robust internal governance structure should be developed to ensure compliance with privacy legislation, including defined roles and responsibilities, policies and practices establishing clear expectations with respect to compliance with privacy obligations, a mechanism to receive and respond to privacy-related questions and complaints, and a commitment to regularly revisiting accountability measures (including bias testing and assessments) based on technological and regulatory developments. The Principles also recommend that an organization undertake privacy impact and/or algorithmic impact assessments to identify and mitigate potential or known impacts of a GenAI

system (or its use) on privacy and other fundamental rights.

6. **Individual Access:**
   The Principles emphasize individuals' right to access and correct the personal information about them that is collected during the use of a GenAI system or that is contained within a GenAI model. Accordingly, an organization must ensure that procedures exist for individuals to exercise such rights.
7. **Limiting Collection, Use, and Disclosure:**
   An organization must limit the collection, use and disclosure of personal information to what is necessary to fulfill an appropriate, identified purpose. The Principles stress that publicly accessible personal information (including personal information published online) cannot be collected or used indiscriminately, including in connection with a GenAI system. Appropriate retention schedules must also be developed for personal information contained within a GenAI system's training data, system prompts and outputs.
8. **Accuracy:**
   Personal information used in connection with GenAI systems must be as accurate, complete and up-to-date as is necessary for the purpose(s) for which it is to be used. This obligation includes, without limitation, identifying and informing users of a GenAI system about any known issues or limitations regarding the accuracy of the system's outputs, and taking reasonable steps to ensure that outputs from a GenAI system are as accurate as necessary for their intended purpose, particularly when the outputs will be used to make (or assist in making) decisions about one or more individuals, will be used in high-risk contexts, or will be released publicly.
9. **Safeguards:**
   Safeguards must be implemented to protect personal information collected or used throughout the lifecycle of a GenAI system from risks of security breaches or inappropriate use. Such safeguards must be commensurate to the sensitivity of the personal information and take into account risks specific to GenAI systems, such as prompt injection attacks, model inversion attacks and jailbreaking.
10. **Considering the Impact on Vulnerable Groups:**
    When developing or deploying a GenAI system, an organization should identify and prevent risks to vulnerable groups, including children and groups that have historically experienced discrimination or bias. GenAI systems should be fair and free from biases that could lead to discriminatory outcomes. For developers, this obligation includes ensuring that training data sets do not replicate or amplify existing biases or introduce new biases. Users of GenAI systems must oversee and review the systems' outputs and monitor for potential adverse effects, particularly when such outputs are used as part of an administrative decision-making process or in highly impactful contexts (e.g., employment, healthcare, access to finance, etc.).

CLICK HERE.

Failure to Train, Discipline, or Supervise Employee Could Lead to A Negligence in Supervision Claim

In a previous blog post, I wrote about the elements of a negligence hiring claim and made recommendations how to avoid liability for your business. A negligence in supervision/retention claim has certain similarities to the negligence hiring cause of action. Negligence hiring, supervision, training, and retention claims are not based on vicarious liability, like a respondeat superior claim. Instead, each of those claims are based upon the actual fault of the employer. G.A.-H v. KGG, 238, N.J. 401, 415 (2019).

To be found liable for negligent supervision, training, or retention, the Plaintiff must establish that: (1) an employer knew or had reason to know that the failure to supervise or train an employee in a certain way would create a risk of harm, and (2) that risk of harm materializes and caused the Plaintiff's damages. DiCosala v. Kay, 91 N.J. 159, 173 (1982). In the employment context, I have seen these claims brought against employers based on the following scenarios:

a. The employer had reason to know that an employee had engaged in unlawful workplace discrimination in the past but decided to retain them; and
b. The employer failed to take affirmative steps such as,
    i. Developing and implementing anti-harassment training
    ii. developing and implementing written policies and procedures that set the expectation that employment discrimination will not be tolerated in the workplace and provide employees with a roadmap for reporting allegedly unlawful behavior.

First, employers can limit their exposure to this claim by not retaining an employee they know or have reason to know has violated employment discrimination laws in the past. If an employee alleges workplace discrimination, the employer has a legal obligation to take steps to ensure that the alleged discriminatory conduct stops. I recommend if one of your

employees makes an allegation of sexual harassment that your company retain the services of a neutral, unbiased, trained investigator to conduct a thorough investigation of the alleged conduct. The investigator will make certain recommendations after their investigation. I strongly encourage your business to follow those recommendations. For example, if the investigator recommends the termination of the alleged perpetrator's employment, your company should do the same. If the company does not follow that recommendation and sometime later, the employee allegedly sexually harasses another employee, the decision not to follow the recommendation of the investigator could result in your company being sued for negligence in supervision, retention, or training.

Second, employers can limit their exposure to this claim or an indirect employment discrimination lawsuit by providing all employees with yearly training and implementing robust policies and procedures to ensure the same. I recommend that training begin at the inception of employment and continue at least once per year. Moreover, I recommend that your company draft and circulate an employee handbook that provides simple, straightforward information about your company's discrimination rules and policies. Those polices should remind employees and managers about their rights, duties, and responsibilities to prevent workplace discrimination. Furthermore, they should educate employees on what to do if they either witness or are subjected to workplace discrimination.
CLICK HERE.