Monthly Newsletter: September 2023

FEDERAL DEVELOPMENTS

EEOC Issues Federal Workforce Reports Focused on Workers with History of Arrest or Conviction

The U.S. Equal Employment Opportunity Commission (EEOC) today released two companion reports examining the federal employment of workers with arrest or conviction records. The EEOC developed these reports in support of President Biden's Executive Order 14035, which calls for the expansion of federal employment opportunities for individuals with arrest or conviction records and requires the evaluation of barriers to federal employment faced by these individuals. These reports show that federal agencies are hiring qualified individuals with prior arrests or convictions in their background checks.

"It is our hope that the information contained in these reports will assist federal agencies in understanding long-standing challenges that the persons with arrests and convictions face when trying to obtain life-changing employment," said Dexter Brooks, associate director of the EEOC's Office of Federal Operations. "As the nation's largest employer, the federal government is uniquely positioned to demonstrate how to improve opportunities for this underserved community."

The first report, *Second Chances Part I: Federal Employment for Workers With Past Arrests or Convictions*, explores how likely workers with prior arrests or convictions were to work in the federal sector and whether "ban-the-box" laws that govern the timing of background checks during the recruiting process better protect applicants from discrimination. The main findings of this report include:

- Between 2003 and 2017, respondents who had been previously incarcerated were about half as likely to be employed in the federal sector compared to those without records. Data is lacking to explain that shortfall.

While it is possible that hiring managers are less likely to hire applicants with any kind of incarceration, conviction, or arrest record, it is also possible that the shortfall is the result of a belief, at least in part, by individuals with arrest and conviction records that the federal government may not hire them.

- Delaying inquiry into arrest and conviction records until later in the recruiting process may make it easier to root out unlawful discrimination. "Ban-the-box" laws and policies prohibit criminal background checks until after a conditional job offer is made. Following implementation of ban-the-box laws for state and local public employers, more workers filed EEO complaints and the EEOC found reasonable cause to believe that discrimination had occurred in more of those complaints.
- Additional research and data are necessary to assess policies that facilitate federal employment for formerly incarcerated workers and those with prior arrests and convictions. This report provides a roadmap for additional research, which led to the second report.

The second report, *Second Chances Part II: History of Criminal Conduct and Suitability for Federal Employment*, examines how often background investigations for federal employment found criminal conduct issues and how often investigations with criminal conduct issues received an unfavorable suitability determination. Suitability determinations are conducted to consider whether a person's character or conduct may have an impact on the integrity or efficiency of federal service, and they decide whether the person is suitable for federal employment. The main findings of the second report include:

- Between fiscal year (FY) 2018 and FY 2020, 22.3% of suitability investigations for federal civil service positions identified criminal conduct issues.
- When criminal conduct was identified as an issue for a civil service position, 76% of determinations were favorable, allowing the candidate to work in the federal government. Only 2% were unfavorable, leading to actions such as not hiring the job candidate or removing the applicant from their current position after starting.
- When criminal conduct was identified as an issue for a civil service position, applicants and appointees were more likely to withdraw their applications, resign, or be removed from their position before an adjudication determination was made (21.7% vs. 14.5% of all civil service cases).

"Persons with arrest and conviction records who have rehabilitated and present a low risk for recidivism need opportunities for stable employment," said Brooks. "Employment in the federal government may help address some of the barriers these individuals face and ease their reintegration into society.

Federal equal employment opportunity laws do not prohibit the consideration of arrest or conviction records in making employment decisions unless doing so results in discrimination based on race, national origin, or another protected category. The EEOC has issued multiple policy statements on the appropriate consideration of arrest or conviction records in employment decisions. The most recent and comprehensive of these documents is Enforcement Guidance, Consideration of Arrest and Conviction Guidance in Employment Decisions under Title VII of the Civil Rights Act. It clarifies how an employer's use of an individual's criminal history in making employment decisions may violate the prohibition against employment discrimination prohibited by Title VII.

The EEOC advances opportunity in the workplace by enforcing federal laws prohibiting employment discrimination. More information is available at www.eeoc.gov.

Click Here for the Original Article

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

State Data Breach Notification Laws – September 2023

While most state data breach notification statutes contain similar components, there are important differences, meaning a one-size-fits-all approach to notification will not suffice. What's more, as data breaches continue to rise, states are responding with increasingly frequent and divergent changes to their statutes, creating challenges for compliance. Organizations must make it a priority to monitor these changes to prepare for and respond to data breaches.

Please click on the link below for full Chart for more information.

Click Here for the Original Article

Delaware Becomes 12th US State to Enact Comprehensive Data Privacy Law

The Delaware Personal Data Privacy Act (DPDPA) takes effect January 1, 2025. Delaware generally followed the Connecticut model, but has some unique terms. We provide a non-exhaustive list of some of Delaware's requirements here.

A lower threshold for application; no categorical exemption for all nonprofits. The DPDPA applies to organizations that control or process personal data of 35,000 or more Delaware residents in a given year or organizations that control or process personal data of 10,000 or more Delaware residents and derive more than 20% of their gross revenue from the sale of personal data. Like states other than California, the DPDPA will only apply to personal data processed for a personal or household purpose (i.e., not in the employment context or in a commercial context). Nonprofits are not categorically exempt from the DPDPA unless dedicated exclusively to preventing and addressing insurance crime.

A broader definition of sensitive personal data. Sensitive data under the DPDPA includes "status as transgender or nonbinary" and "mental or physical health condition or diagnosis (including pregnancy)."

Protection for teens. Entities subject to the DPDPA cannot, without consent, sell or process for targeted advertising purposes the data of consumers that the entity knows, or willfully disregards, that the individual is between the ages of 13 to 18.

Additional data access rights. The DPDPA gives Delaware residents the specific right to "obtain a list of the categories of third parties to whom the controller has disclosed the consumer's personal data." This is similar to one part of California's right to know about categories of information.

Right to cure with sunset. The DPDPA provides a 60-day cure period for violations, which sunsets on December 31, 2025.

No private right of action. The DPDPA contains no private right of action; it will be exclusively enforced by the Delaware Department of Justice.

Click Here for the Original Article

New York makes wage theft a crime

Over the past decade-plus, New York lawmakers have passed several laws intended to combat perceived wage theft across the Empire State. On September 6, 2023, lawmakers in Albany continued this trend by passing a bill that codifies wage theft as criminal larceny.

Specifically, the bill adds a new subsection to the New York Penal Law's larceny statute to include wage theft, which it describes as when a person is hired "to perform services and the person performs such services and the [employer] does not pay wages, at the minimum wage rate and overtime . . . to said person for work performed." In such a case, the prosecution is permitted to aggregate multiple non-payments or underpayments from an individual or workforce, even if such incidents occurred in multiple counties.

Simply put, New York State employers who fail to timely and fully pay all wages due to their employees could potentially now be subject to criminal penalties (in addition to the preexisting civil damages and penalties).

Click Here for the Original Article

COURT CASES

FTC Settles With Background Report Companies for FCRA Violations and Deceptive Acts

The Federal Trade Commission ("FTC") on September 11, 2023, settled a claim against a group of affiliated entities operating a background reporting business, Instant Checkmate, LLC, TruthFinder, LLC, The Control Group Media Company, LLC, Intelicare Direct, LLC, and PubRec LLC ("background report companies" or "companies") for alleged misrepresentations that deceived consumers about whether they had criminal records and for operating as a consumer reporting agency without following the requirements of the Fair Credit Reporting Act ("FCRA"). The companies were ordered to pay a $5.8 million civil penalty, which the companies are jointly responsible for.

The FTC found that the background report companies violated the FTC Act's prohibition against unfair and deceptive acts by sending notifications and emails to users of their websites that indicated that the subject of a background report had a criminal or arrest record, when the individual actually had a traffic ticket. The companies then charged consumers monthly subscriptions fees to view the full background reports. The companies also deceived consumers into thinking they could dispute or remove inaccurate information, by providing "remove" and "flag" buttons that only removed the information from that consumer's view, but not from the actual report.

The FTC found that the companies violated the FCRA by operating a consumer reporting agency without taking any steps to ensure the accuracy of the reports they provided and by providing reports to people who did not have a permissible purpose to view the reports.

The final order requires the companies to, among other things:

- Establish and implement a comprehensive monitoring system to assess and determine to what extent the company is operating a consumer reporting agency
- Maintain reasonable procedures designed to limit the furnishing of consumer reports to persons with permissible purposes to receive them and that appropriate FCRA notices are provided to consumers
- Maintain procedures to assure the maximum possible accuracy of the information concerning consumers about whom reports relate
- Provide accurate representations regarding the effect of removing or flagging inaccurate consumer report information, and provide accurate representations about whether information in a report relates to a criminal record

This is the second FTC settlement against Instant Checkmate, which settled a claim in 2014 for alleged previous violations of the FCRA. Again, in that case, Instant Checkmate failed to take reasonable steps to make sure that its background reports were accurate and that its users had a permissible purpose to have them.

Click Here for the Original Article

Illinois Court Eliminates Another BIPA Defense

This summer, the U.S. District Court for the Southern District of Illinois further bolstered Illinois' Biometric Information Privacy Act's (BIPA) nearly unfettered private right of action in *Lewis v. Maverick Transportation*. In a simple but firm four-page ruling, Judge Rosenstengel denied the defendant's motion to dismiss, holding that a cause of action under BIPA does not require a plaintiff to plead that data collected is used for identification purposes. The ruling serves to highlight the apparent lack of any real technical defenses to the statute — making it imperative that companies focus on strict compliance before they find themselves in court.

Background

BIPA is a privacy statute that prohibits, among other things, the collection and dissemination of biometric data without consent. To effectuate this goal, BIPA regulates the collection, use, safeguarding, and storage of biometric information and biometric identifiers such as fingerprints, retina scans, or face scans — also known as "biometric information." Under BIPA, private entities in possession of biometric information are required to: (1) develop a written policy governing management of the biometric information; (2) inform the owner of the biometric information; and (3) obtain consent from the employee to gather the biometric information.

Due to the uniquely plaintiff-friendly contours of the statute, courts have seen a panoply of putative class actions, leaving countless companies scrambling to develop workable defenses. This summer, the Southern District of Illinois eliminated one of those efforts.

Lewis v. Maverick Transportation

In its motion to dismiss, the defendant, *Lytx*, which provides video and analytic services — such as its DriveCam — to the transportation industry, argued that the plaintiff failed to adequately plead a BIPA claim because he did not allege that the captured information was used for identification purposes. In asserting this argument, the defendant relied on the BIPA statute's text, which defines biometric information as "any information…used to identify an individual." Because BIPA exclusively regulates biometric identifiers and biometric information, the defendant presumed that failing to allege that such information had actually been used to identify the plaintiff represented a fatal flaw in the pleading. In short, the defendant argued that BIPA requires plaintiffs to plead that the collected information is used to identify them.

The Southern District disagreed. Relying on dicta from the District of New Jersey and the Seventh Circuit, the court determined that, contrary to the defendant's arguments, "BIPA does not require a plaintiff to plead that the collected information is used to identify them." In so doing, the court reasoned that the purpose of BIPA is not to ensure *how* an individual's information is used (*i.e.*, to identify them) but rather "to ensure that consumers understand, before providing their biometric data, how that information will be used, who will have access to it, and for how long it will be retained."

Significant Trend

This ruling signals a stark and significant trend for BIPA litigation — particularly in light of two BIPA decisions issued in the spring of 2023. On February 2, the Illinois Supreme Court held that a five-year statute of limitations period applied to all sections of BIPA, partially reversing a previous ruling by the Illinois Appellate Court, which held that a one-year statute of limitations applied in certain instances.[1] Then, on February 17, the Illinois Supreme Court held that a claim is triggered upon each biometric scan rather than just the first — vastly compounding the potential damages available to plaintiffs.[2] Based on this recent spate of rulings, it is evident that neither the courts nor the legislature intend to make life easier for defendants in the near future. Instead, defendants are seeing their exposure increase and their arguments deemed ineffective.

Takeaway

Private entities collecting biometric information must be more vigilant than ever in their efforts to comply with BIPA. Indeed, the exposure that BIPA presents is too significant to risk litigation, particularly when that risk relies on textual interpretation of the statute. Time and again, the courts have made clear that there will be no respite for defendants on the horizon. Given the apparent lack of any technical defenses to the statute, private entities must institute policies and practices that satisfy the statute's strictures and should engage counsel to ensure full compliance before litigation becomes inevitable.

Click Here for the Original Article

INTERNATIONAL DEVELOPMENTS

UK bolts US 'data bridge' deal onto EU-US Data Privacy Framework

The U.K. government has officially confirmed it will piggyback on a transatlantic data transfer deal between the European Union and the U.S. by bolting on an extension that is dubbed the "U.K.-U.S. data bridge."

Back in June, the U.K. and U.S. reached an agreement in principle over this arrangement. Today the U.K. government confirmed that secretary of state, Michelle Donelan, has moved forward with the deal — which is intended to grease digital commerce by allowing for U.K. citizens' information to be exported to the U.S. under an assurance of adequate levels of protection for people's information, in line with the UK's data protection regime (aka the U.K. GDPR), once it's over the pond.

"The Secretary of State has determined that the UK Extension to the EU-US Data Privacy Framework does not undermine the level of data protection for UK data subjects when their data is transferred to the US. This decision was based on their determination that the framework maintains high standards of privacy for UK personal data," the DSIT wrote today.

"Supporting this decision, the US Attorney General, on September 18, designated the UK as a 'qualifying state' under Executive Order 14086. This will allow all UK individuals whose personal data has been transferred to the US under any transfer mechanisms (i.e. including those set out under UK GDPR [General Data Protection Regulation] Articles 46 and 49) access to the newly established redress mechanism in the event that they believe that their personal data has been accessed unlawfully by US authorities for national security purposes."

The U.K.-U.S. data bridge — aka the "UK Extension to the [EU-US] Data Privacy Framework" (DPF) — will enable U.S. companies that are certified under the EU framework to sign up to be able to receive U.K. personal data through the DPF.

While Donelan's decision to grease the flow of U.K. to U.S. data will be cheered by many as the sane and rational thing to do, unpicking another of Brexit's myriad harms, the U.K. building its U.S. data bridge atop the EU's framework does raise questions over the durability of the arrangement given the DPF is set to face legal challenge in the EU.

Data protection experts argue it does not protect the bloc's citizens' data to the required equivalent level. And the prior two EU-U.S. data transfer deals were struck down by the bloc's top court, in 2015 and 2020. If a third strike were to bring the DPF tumbling down, one question would be what happens to the U.K.'s bolt on arrangement?

Albeit, since the EU court of justice no longer has jurisdiction in the U.K., it's possible the U.K.'s bolt on extension bridge might just be the only bit that survives. Not least because the U.K. government is also in the midst of watering down domestic privacy standards . . . 😐

The U.S. bridge is not the first data sharing deal the U.K. has inked post-Brexit; that was the adequacy decision it took back in July 2022 with South Korea.

Click Here for the Original Article

India Passes Privacy Law

India—the fifth largest economy in the world—just passed a comprehensive privacy law. On August 11, 2023, the Digital Personal Data Protection Act, 2023 (the "DPDP") was approved by the president of India, adding India to the list of global powers with a comprehensive privacy law. The law is expected to come into force in June 2024. Guest author Stephen Mathias, from Kochhar & Co., provides a detailed breakdown of the DPDP.

Like other major privacy laws, the DPDP has an extraterritorial reach: it applies to the processing of digital personal data outside India,[1] if the processing is in connection with any activity related to the offering of goods or services to individuals within India. Thus, even if a company's operations are not physically in India, it may still be subject to this law. Fortunately, for global companies that are already subject to the European Union General Data Protection Regulation ("GDPR") and the many comprehensive privacy laws in the United States, the DPDP can be harmonized with existing compliance programs. The new law shares many provisions with existing privacy laws, such as obligations to honor data privacy rights (access, correct, delete, redress, and opt-out), provide a privacy notice, protect personal data, provide notice of a data breach, enter into contracts with processors, and limit retention of personal data.

However, companies should note some of the differences between the DPDP and other privacy laws when conducting a gap analysis and developing policies and procedures to bridge those gaps. For example, unlike both the GDPR and US privacy laws, the DPDP places obligations on data subjects/consumers (called "data principals" under the DPDP). Further, unlike US privacy laws, the DPDP also has requirements relating to data transfers, data protection officer appointment and lawful basis for processing. Finally, unlike the GDPR, the DPDP is primarily a consent-based privacy law; processing in the absence of consent is possible for certain limited "legitimate uses," such as to fulfil legal or judicial obligations, or for the purposes of employment. That said, the DPDP's consent-based lawful basis for processing aligns with the growing trend in the European Union to obtain consent for certain processing activity, such as advertising and marketing, instead of relying on other grounds, following recent case law of the Court of Justice of the European Union in this respect.

Failure to comply with provisions under the DPDP may lead to fines of up to INR 250 crores (approximately USD 30 million).

For an overview of the similarities and differences among these laws, we provide the chart below.

Party Names

	India	EU	US[2]
Determines Purposes and Means of Processing	Data Fiduciary & Significant Data Fiduciary *(per government notice)*	Controller	Controller/Business
Processes Data For Another	Data Processor	Processor	Processor/Service Provider/Contractor
Individual to Whom Data Relates	Data Principal	Data Subject	Consumer

Data Principal Rights

	India	EU	US
Access	✓	✓	✓
Data portability	✗	✓	✓
Delete	✓	✓	✓
Correct	✓	✓	✓
Opt-out/object	✓	✓	✓
Not to be subject to profiling/automated decision making	✗	✓	✓
Additional rights around sensitive data	✗	✓	✓
Appeal/redress	✓	✓	✓

Data Principal Obligations

	India	EU	US
Comply with applicable law	✓	✗	✗
No impersonation of another person	✓	✗	✗
No suppression of material information	✓	✗	✗
No false or frivolous grievance or complaint	✓	✗	✗
Furnish verifiably authentic information	✓	✗	✗

Data Fiduciary Obligations

	India	EU	US
Lawful basis for processing	✓	✓	✗
Data transfer requirements	✓	✓	✗
Contracts with processors	✓	✓	✓
Privacy policy	✓	✓	✓
Security and breach notification	✓	✓	✓
Data retention limitation	✓	✓	✓
Appoint data protection officer	✓	✓	✗

Click Here for the Original Article

Member of French Parliament lodges first request for annulment of EU-US Data Privacy Framework

Latombe, who is not only a Member of the French Parliament, but also seated at the French Data Protection Authority (CNIL)'s Commission, lodged a request for annulment of the DPF on 6 September 2023 before the Court of Justice of the European Union (CJEU). Latombe, however, specified in his press release that he is acting "in a personal capacity, as a simple citizen of the Union, and not as a French MP, Law Commissioner or CNIL Commissioner."

Latombe's request, reportedly spanning 33 pages and accompanied by numerous annexes, is based on Article 263 of the Treaty on the Functioning of the European Union (TFUE) that states that "Any natural or legal person may, under the conditions laid down in the first and second paragraphs, institute proceedings (…) against regulatory acts which directly concern them and which do not involve implementing measures".

Admissibility of the request

The first step for the CJEU will be to analyse whether Latombe's request is admissible. Indeed, as he is acting as an individual, he qualifies as a "non-privileged applicant", which means that he is subject to stringent conditions to satisfy the legal standing requirement for his request to be admissible.

Based on the CJEU caselaw, he will need to demonstrate that the DPF is both of direct concern (CJEU Case C-486/01 Front national v. European Parliament) and of individual concern (CJEU Case C-25/62 Plaumann v. Commission) to him.

If both requirements of direct and individual concerns are met, although the individual concern criteria seems difficult to demonstrate here, the procedure will offer the advantage of speed compared to the prejudicial question procedure used by Maximilian Schrems (see our coverage of the Schrems cases, here).

Content of the request

Latombe used the main following legal arguments:

- Effective remedy: Latombe is criticizing in his request the absence of guarantees of a right to an effective remedy, and in particular the lack of transparency in the newly created Data Protection Review Court (DPRC) procedure.
- Minimization and proportionality principles: He is also raising the argument of the breach of the minimization and proportionality principles of the GDPR, in particular due to what he identifies as “bulk collection of personal data” by the U.S. surveillance authorities.
- Languages: Latombe also makes a point regarding the language of the DPF decision, that is for now only available in English, but should also be translated into the official languages of the European Union (EU).

The forthcoming decision by the CJEU, both in terms of admissibility and substance, promises to wield a major impact. It will become another cornerstone in the evolving case law in this field, marking a crucial point in transatlantic data transfers.

Click Here for the Original Article

Data Privacy Laws Comparison: Indian DPDP vs. GDPR vs. CCPA

S. No	Principle	European Union General Data Protection Regulation (GDPR)	California Consumer Privacy Act, 2018 (CCPA)	Digital Personal Data Protection Act, 2023 (DPDPA)
1	**Applicability and Extra-Territoriality**	The GDPR applies to: (1) individuals that are EU residents, (2) organisations that are based in the EU, or (3) organisations based outside the EU, that target EU citizens.	The CCPA protects California residents and applies to organizations that are doing business in California.	The DPDPA applies to all processing of digital personal data that occurs (a) *within India*; as well as (b) *outside India* in relation to any activity relating to the offering of goods or services to data principals in India.
2	**Types of Data Protected**	The GDPR applies to ***'processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.'***	The CCPA maintains a broad definition of "personal information" or PI, referring to it as ***"information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."***	The DPDPA applies to **digital personal data**. Personal data under the Act refers to ***data about an individual who is identifiable either by such data or in relation to such data.***
3	**Data Processing**	Processing of EU personal data may only be undertaken if the controller has a **lawful basis for processing** under the GDPR.	The CCPA provisions apply to "collecting" personal information and some apply to "selling" or sharing it. The provisions of the Act primarily apply to these three activities.	The term *'processing'* has *wide* import under the Act. It extends to all automated operations (whether wholly or in part) performed on digital personal data, and includes the collection, recording, organisation, storage, retrieval, use, indexing, sharing, erasure and destruction of such personal data.
4	**Consent**	The basic requirements for the effectiveness of a valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR. **Consent must be freely given, specific, informed and unambiguous.** In order to obtain freely given consent, it must be given on a voluntary basis. The element "free" implies a real choice by the data subject.	The CCPA defines that **consent should be a specific, freely given, specific, informed and unambiguous indication of the consumer's intent.**	Consent under the DPDPA is defined as an indication by the data principal signifying an agreement for their data to be processed for a specified purpose. **Consent should be free, specific, informed, unconditional and unambiguous and it should be through clear affirmative action.**
5	**Data Processing of Children**	Article 8(1) of the GDPR sets an age limit for child with respect to processing of personal data. **The processing of personal data of a child shall be lawful where the child is at least 16 years old.** However, if the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.	The CCPA extend privacy protections to California residents of all ages, including minors. Businesses operating in California must provide notice to consumers, including parents or guardians of minors, about the collection and use of sensitive personal information. When it comes to children's data, the CCPA requires businesses to obtain affirmative authorization or opt-in consent to sell the data of a person under the age of 16. Subject to consent requirements, the handling of children's data is covered under the three primary activities of collecting, selling and sharing delineated under the Act.	**Processing the personal data of children and disabled persons with guardians** creates **additional obligations under the DPDPA.** The Act defines a child as an individual under the age of 18. Consent of parent or guardian is needed to process data of such categories of persons.
6	**Rights of Data Principal/Data Subject/ Consumer**	The GDPR outlines 8 fundamental data subject rights, plus the right to withdraw consent, which guarantees individual autonomy over both personal data and its processing. These are mentioned below: 1. Right to be informed 2. Right to access 3. Right to rectification 4. Right to be forgotten/Right to erasure 5. Right to data portability 6. Right to restrict processing 7. Right to withdraw consent 8. Right to object 9. Right to object to automated processing	The rights of consumers under the CCPA can be classified as follows: 1. Right to Notice 2. Right to Access 3. Right to Opt-Out 4. Right to Request Deletion 5. Right to Equal Services and Prices	Data principals have certain rights with respect to their personal data 1. Right to access 2. Right to correction and erasure 3. Right to nominate 4. Right of grievance redressal 5. Duties of data principals

7	**Obligations of Data Fiduciaries/Controller**	Data Controllers are responsible for the strictest levels of GDPR compliance. According to Article 24 of the GDPR, they must actively demonstrate full compliance with all data protection principles.	Business entities have several obligations that they must comply with while handling consumer data under the CCPA. Provided below are a few key obligations under the CCPA: 1. Provide Do Not Sell Button 2. Opt-in Minors 3. Provide Privacy Notices 4. Limit Collection and Use 5. Provide Access 6. Delete PI upon request 7. Non-Discrimination 8. Reasonable Security Precautions	**Data fiduciaries** are responsible for complying with the following obligations: 1. Take consent for data processing activities. 2. Notify personal data breaches. 3. Apply technical safeguards and reasonable security measures. 4. Not over-retain personal data. 5. Appoint a grievance officer. **Significant Data Fiduciaries:** In addition, are required to: 1. Appoint a Data Protection Officer 2. Appoint an independent data auditor. 3. Undertake data protection impact assessments (DPIA), and periodic audits.
8	**Cross-Border Transfer**	Chapter V of the GDPR devotes an entire chapter to cross-border personal data transfers . Sanctions for breaching data protection rules are severe: the penalty for cross-border transfer violations is up to €20 million, or up to 4% of the annual global turnover of the preceding fiscal year, whichever is higher.	The CCPA, which is essentially a state law, doesn't regulate the transfer of personal information across international borders, but does overlap and possibly conflict with certain GDPR cross-border transfer restrictions.	The DPDPA abandons the white list approach of the 2022 Bill and instead adopts a negative list. Essentially, data can be transferred to all countries outside of those barred by the Central Government by way of notification. Sectoral restrictions on data transfers such as those of the RBI will continue to apply.

Click Here for the Original Article

Quebec's Privacy Law

The bulk of Quebec's privacy law, Law 25, is set to be in effect on September 22. Law 25 was passed on September 22, 2021, with implementation coming into effect over the course of three years – and this September marks the effective date for many of its core requirements. Quebec passed this law in the wake of continuous attempts at a general overhaul of Canada's privacy regime to be more in line with modern privacy legislation inspired by the EU's General Data Protection Regulation (GDPR). Law 25 is the first provincial law in Canada to mimic such GDPR requirements.

As September 22 approaches, below are some key points on what should be on your radar to comply with Law 25:

- ***Who's In Charge?***: Law 25 has required the appointment of a "person in charge of the protection of personal information" since September 2022. This is the functional equivalent of what we have come to known as a Data Protection Officer (DPO) under laws like the GDPR. Note that Law 25 suggests that this person in charge of the protection of personal information (including administrators, directors, or representatives of the company who ordered or authorized an act or omission constituting an offense under Law 25) can be held personally liable.
- ***What is Personal Information?***: Quebec defines personal information broadly, just like the GDPR, as it includes any information that allows a person to be identified – including consumer, employee, and business to business personal information. Note that this differs from what we see from many US state privacy laws which exempt employee and business to business personal data from the ambit of the law.

- ***Quebec Resident Rights***: Similar to other privacy laws, Law 25 gives Quebec residents certain privacy rights. This includes the right to: be informed, access, rectify, erase, withdraw consent/restrict processing, and opt-out of profiling. Law 25 provides businesses with 30 days to respond. Note that the right to portability will be implemented in September 2024.
- ***Contractual Requirements***: Law 25, like GDPR and other comprehensive privacy laws, requires contractual language to be in place when disclosing personal information with processors like your service providers. Contracts should include restrictions on use of the personal information, ensure proper security measures are in place, and account for deletion of information upon expiration of the contract.
- ***Expanded Risk Assessment Triggers***: Law 25 mandates the completion of a risk assessment (similar to GDPR data privacy impact assessments) in certain situations, including those not required under other privacy laws. One notable time where a risk assessment is required is any time personal information may be transferred outside of Quebec. Amongst other factors, a risk assessment should contain a review of the processing activity, relevant safeguards set forth to protect the personal information, and an analysis of the legal framework of the country the information is being transferred to.

Quebec's law also requires additional compliance measures – such as keeping a record of all breaches, even those that do not trigger notice requirements, providing disclosures relating to use of automated decision-making, and obtaining consent for the use of tracking technologies such as cookies. Law 25 will intertwine with other Quebec legal requirements, such as ensuring all notices, legal documents, and materials are available in French. Compliance with Quebec's Law 25 should be taken seriously as it provides for both a private right of action and enforcement by the CAI for penalties of up to $25 million CAD or 4% of your company's global turnover.

So What Should My Company Do Now? First, determine whether your organization is subject to the law – do you collect Quebec residents' personal information? If the answer is yes, the good news is that many of Quebec's requirements are familiar to companies already in compliance with laws like the GDPR and CPRA. You should work with legal counsel to update your privacy policies to ensure proper disclosures and privacy rights are provided for, update internal documents and DPAs, and set up processes to ensure risk assessments are conducted when needed.

Click Here for the Original Article

MISCELLANEOUS DEVELOPMENTS

Employment law differences between Canada and the U.S.

Read this if: you are hiring a cross-border team and need to review U.S. and Canadian employment laws

You might also like: Cross-border funding for startups: key questions founders should ask

Go deeper: Going cross-border

If you hire team members from Canada and/or the U.S., you must ensure that you meet local employment law standards, regardless of where your startup's head office is located. We break down the key differences in employment law between the two jurisdictions.

Discrimination

In Canada and the U.S., discrimination in employment is prohibited on specified grounds, such as race, gender, ethnic origin, religion (creed), and age. Discrimination due to sexual orientation is prohibited across Canada and several (but not all) states in the U.S.

The most significant differences between the two countries relate to discrimination based on disability.

In Canada, disability-based discrimination is prohibited under human rights codes and the *Canadian Charter of Rights and Freedoms*. Employers have a duty to accommodate an employee's disability up to the point of undue hardship to the employer. This means that a Canadian employer must accommodate their employee's disability up to the point where the solution would be deemed to present too high a health and safety risk, or too high a cost to implement, therefore going above the "reasonableness standard". This is determined on a case-by-case basis.

Workplace drug and alcohol testing is generally restricted in Canada, and alcoholism and drug addiction are legally recognized as disabilities that require accommodation.

In the U.S., disability-based discrimination is prohibited under the *Americans with Disabilities Act*. Employers must provide reasonable accommodations to a disabled employee, unless doing so would cause undue hardship to the employer. Determining the "reasonableness standard" is done on a case-by-case basis, however some states have expanded the definitions of covered disabilities and reasonable accommodation in a bid to provide more uniformity across the court's decisions.

Workplace drug and alcohol testing are much more common in the U.S. and are generally legally permissible, although the requirements vary by state—with some allowing random testing whilst others limit tests to circumstances involving "reasonable suspicion" or "probable cause". Alcoholism and being in recovery from drug addiction are recognized as disabilities.

Restrictive covenants

Restrictive covenants are clauses that are put into an employment agreement to restrict employees, or ex-employees, from carrying out acts that could harm the business after they cease to be employed. The two most challenging post-employment restrictive covenants in employment agreements are non-competition and non-solicitation clauses.

Non-competition clauses act to prevent employees from leaving their current job to work with, or launch, a business that is a direct competitor. Non-solicitation clauses are put in place to stop ex-employees from soliciting your team or customers to join them at a new company. When deciding if a clause is enforceable, the courts will assess, among other things, if its restrictions are set out for a reasonable time, if the geographic scope is clearly defined and fair, and if it was in relation to a protected business activity.

In Canada, non-compete clauses are presumptively unenforceable, except in limited circumstances (i.e., Canadian courts usually only enforce them for high-ranking employees such as C-suite executives), with the province of Ontario prohibiting employers from entering into a non-compete agreement with employees below the executive level.

Courts across Canada are generally more receptive to enforcing non-solicitation clauses, if they determine the clause was clearly and unambiguously drafted. Canadian courts do not modify restrictive clauses, so one that is vague or too broad will be struck out completely.

In the United States, the enforceability of restrictive clauses is dependent on state law. Courts in most states will generally enforce non-competition agreements if the clause is determined to be for a reasonable time and geographic scope. U.S. courts will also look to ensure that the restrictions are no greater than is necessary to protect the employer's legitimate business interests. For states that deem non-competition clauses unenforceable, it is usually due to public policy reasons. However, the FTC has proposed a rule that would effectively invalidate any non-compete agreements, superseding the current patchwork laws in place.

As with Canada, non-solicitation clauses are generally allowed. Some states will deem an overly broad restrictive covenant to be unenforceable in its entirety, while others will permit the modification of the terms of the clause, particularly if it contained a note allowing modifications.

Compensation disclosure for public companies

If you go public in either Canada or the U.S., you must publicly disclose the compensation made to founders, CEOs, and other high-ranking employees.

Shareholders may also vote on the compensation of executives (referred to as “say on pay”), however, how this is approached differs between Canada and the U.S.:

- In Canada say-on-pay is still voluntary, although the prevalence of say-on-pay is increasing among large public issuers.
- In the U.S., a non-binding shareholder vote on compensation (say-on-pay), as well as a vote on the frequency of say-on-pay, is mandatory.

Tax on options

In both countries, option holders are generally taxed when exercising stock options (i.e., purchasing shares per the stock option agreement). The amount they are taxed on is the difference between the fair market value of the stock on the date of exercise and the exercise price. The key difference between the tax on options in Canada vs the U.S. centers on who receives tax advantages.

In Canada, once certain requirements are met, the option holder receives a tax advantage as the spread is taxed at capital gains rates. The company is not entitled to a tax deduction in respect of the issuance of shares when an option is exercised.

In the U.S., options are typically designed either as incentive stock options, with the potential for preferential tax treatment, or as nonqualified stock options subject to ordinary income taxation.

Incentive stock options (ISOs) are not subject to basic ordinary income taxation upon vesting or exercise, and the employer cannot take a corresponding compensation deduction. Although ISOs have fallen out of favor in many industries in the U.S., due to statutory constraints and administrative complications, they remain prevalent in the startup ecosystem as they offer employees a more favorable tax result than nonqualified stock options.

Nonqualified stock options (NQSOs) allow the holder to recognize ordinary income in an amount equal to the option spread, and the employer is generally entitled to a corresponding tax deduction.

Tax on restricted stock

Restricted stocks are employee stocks that are placed under a vesting schedule. This means that a specified amount of time must pass before restrictions on accessing the stocks are lifted and the employee can transfer their shares to a third party, a bank, etc.

In Canada, employees are taxed on restricted stock at the time that they are granted it. If a Canadian employee would prefer to be taxed via ordinary income rates when the restrictions have lifted (which is like the U.S. approach), then the company must grant the employee restricted share units instead. These are notional units whose value is equivalent to the company's shares. However, restricted share units have deferral or deductibility limitations depending on the structure chosen and whether the restricted share units are settled in treasury shares, cash, or shares purchased on the open market.

In the U.S., as mentioned above, restricted stock is taxed via ordinary income rates at the time the restriction lapses, unless the employee decides to state the stock as income within 30 days of being granted it. After that, the shares are eligible for short- or long-term capital gains treatment. Share units can also be granted in the U.S. and are a relatively common form of equity incentive.

Termination of employment

In Canada, employment standards legislation requires you to give employees at least the statutory minimum amount of notice of termination or pay in lieu when they are dismissed "without cause". In Ontario, you may also have to pay the terminated employee statutory severance pay. These amounts cannot be contracted out of and cannot be conditioned on a release.

In some cases, you may also be required to give lengthier notice, or pay in lieu, under common law, civil law, or the employee's employment agreement. Termination payments in excess of the statute can be conditioned on a release of claims.

In the U.S., employment is generally "at will", which means an employee can be terminated at any time without cause. Generally, notice of termination is required only if it was included in the employment contract or is company policy.

Severance policies

Severance pay is compensation that an employer pays to an employee whose employment with the company is being terminated through no fault of the employee (i.e., they were not fired due to their behaviour/actions).

In Canada, plans and policies are uncommon, because they usually cannot override an employee's legal rights to notice of termination. In circumstances where severance does come into play, notice and entitlements are generally determined on an individual basis.

In the U.S., severance policies are more common, with the benefits they provide usually tied to seniority and/or length of service. Many U.S. employers do not maintain a formal, written severance policy. Instead, severance determinations are made on a one-off basis depending on the value related to the claims released by the employee in exchange for the severance payment. Companies will also sometimes establish severance policies for limited windows of time in connection with layoffs or reorganizations.

Employment litigation

Wrongful dismissal litigation in Canada is well-developed and tends to result in more predictable damage awards. As a result, it may proceed more quickly to resolution than in the United States.

In the United States, employment litigation against employers can include claims of discrimination under state or federal law. While wrongful termination litigation in the United States has gained a reputation for unpredictable damage awards resulting from jury trials, most cases settle out of court.

Click Here for the Original Article