EVERSHEDS SUTHERLAND

Global Biometrics Guide 2022

A multi-jurisdictional look at the laws governing the use of biometric technology

Contents

Preface

Frank Nolan, Editor

Frank is a Partner in the New York office of Eversheds Sutherland (US) LLP

As any fan of Sherlock Holmes can attest, identifying a person through their unique biological characteristics, such as fingerprints, is nothing new. Harnessing the power of cutting-edge technology and Artificial Intelligence (AI) to leverage an individual's inherent physical and behavioral traits is, however, another story altogether.

Over the last 15 years, biometric technology has hit the mainstream, exploding into a multibillion-dollar industry and touching nearly every aspect of modern life. Whether through a simple finger scan to unlock a phone, access a bank account, move ahead of a queue or gain entry to a secure work area, or via a facial recognition scan as they move through a crowd, most people have provided their biometric information to a private entity, even if they do not necessarily know about it. The dramatic growth and innovation of biometrics only accelerated during the COVID-19 pandemic, as it became clear early in the crisis that biometrics are uniquely positioned to solve many practical problems that arise in a socially distanced world. As we look toward a post-lockdown world, the biometrics industry shows no signs of slowing.

As is often the case with emerging technology, however, legal questions and hurdles abound. Across the globe, companies that employ biometrics – with their customers, employees and the public at large – must navigate a shifting legal and ethical landscape.

This guide aims to provide an overview of relevant laws, regulations and other considerations for companies operating in many regions around the globe. We begin with the basics.

What are biometrics?

Although the term "biometrics" is defined inconsistently across jurisdictions, it is generally used to describe the technologies, data and processes that can identify an unknown person or verify a known person's identity by reference to their biological and/or behavioral characteristics.

Biometric identifiers include or can be derived from an individual's fingerprint, facial structure, voice pattern, ear canal structure, palm print, vein pattern or iris image. Behavioral identifiers include gait pattern, typing style or the manner in which a subject uses their phone. An increasing number of systems use multiple pieces of biometric data, such as a multifactor authentication system that employs a combination of biometrics and other forms of authentication (such as passwords). Implementation of liveness detection is increasingly common – as its title suggests – to ensure that a subject is an actual person during the biometric verification process, thus increasing the security benefits of biometrics.

Most biometric systems collect an image or replica of a subject's biometric identifier and convert it to a series of letters and/or numbers called a template. (Typically, the scan is simultaneously discarded.) Later, when a subject attempts to access the same system, the subject's biometric data is compared with the stored template or templates to create a confidence score indicating the probability that the subject's biometric data matches a stored template. If that score is high enough, the system will identify the subject or verify their identity, depending on the system's functionality and purpose.

Biometric technology typically records unique physical, factual landmarks of a subject at enrollment, then later compares a candidate's similarly acquired landmarks to determine a statistical match likelihood. Biometrics systems generally employ one or more of three types of comparative tools: 1:1 (comparing a single user to a single stored template), 1:N (comparing a single user to a number of stored templates), or N:N (comparing numerous users to numerous stored templates).

Present and future: Technical advancement and COVID-19

The past few years have seen dramatic innovations in biometric technology and an accompanying exponential growth in the size of the biometrics industry, in part due to the spread of the Internet of Things (IoT), AI and edge computing products into businesses and homes across the globe. Biometrics generally offer numerous benefits for companies and users alike. For example, biometrics can provide a more secure, easier, faster and oftentimes cheaper alternative to traditional passwords. Not surprisingly, nearly every industry has found uses for biometrics, including in transportation, manufacturing, automotive, health care, education, insurance, banking, payments, fashion, real estate and entertainment.

As noted, the global COVID-19 pandemic required even greater development and deployment of biometrics. Private-public sector cooperation in law enforcement, travel and public health expanded, and health passports and the rise in remote work provided new opportunities. The industry has already adapted to a climate where social distancing and avoiding contact with surfaces can be of paramount concerns. Improvements in contactless scanning, iris recognition and voice pattern detection will contribute to what many are expecting to be accelerated growth of the biometrics industry in the near future.

...biometrics can provide a more secure, easier, faster and oftentimes cheaper alternative to traditional passwords.

Legal, social and ethical context

Although business is booming in the biometrics space, the public response has been difficult to gauge. Consumers may feel favorable toward the prospects for seamless and accurate identity verification that biometrics offer, but people can naturally feel more protective of their biometric information than, for example, their names, addresses or other more traditional forms of personal information. It is also fair to say that some biometrics applications have raised concerns that can overshadow more socially acceptable uses of the technology. Perhaps most notably, governmental and police use of facial recognition technology without the consent of citizens has triggered civil rights and privacy questions. Algorithmic bias, unconsented use of subjects' biometric identifiers to construct algorithms, biometric emotion detection, use of voice biometric data to construct an image of the speaker's face and passive behavioral biometrics have also grabbed headlines and, at times, the attention of regulators and lawmakers.

Given the complicated ethical questions and quickly evolving technology, it is unsurprising that lawmakers have struggled to enact workable laws around notice, consent and destruction of biometric data. Depending on the jurisdiction or industry, laws may regulate according to application (such as facial recognition), by technology (AI), by user (government use v. private), by industry or even by level of government (subnational v. national government). Some jurisdictions simply do not regulate the collection, storage and use of biometric data, leaving a void that can or will be filled in one way or another.

Where does this leave companies that wish to abide by relevant legal standards while taking advantage of the many benefits that biometrics can offer their customers and employees? We endeavor to provide guideposts to help answer that question in this global guide to biometrics.

United States

by Frank Nolan and Jessica Rodgers

Frank is a Partner in the New York office, and Jessica is an Associate in the Washington DC, office of Eversheds Sutherland (US) LLP.

The existing state biometrics laws

Only three states have enacted stand-alone legislation specifically addressing commercial collection, storage and use of biometric information. Significantly, none of these laws prohibits the collection, use or storage of biometric information. Instead, the statutes impose varying consent and notice requirements with which most companies must comply. The most well-known and restrictive of these laws is the Illinois Biometric Information Privacy Act (BIPA), which remains the only law of its kind to provide a private right of action.

Several state legislatures have proposed similar laws to BIPA in the past few years, and a growing number of states have incorporated biometrics into their data breach notification statutes. A small number of municipalities, including New York City, the largest city in the country, have also enacted biometrics laws. At the federal level, biometrics are addressed in a few industry-specific regulations, the Federal Trade Commission (FTC) has issued nonbinding guidance and has initiated enforcement actions in this area, and a handful of bills have been proposed in the US Congress. The legal landscape for biometrics in the United States remains unsettled.

Because the Illinois BIPA law is the most robust statute, and one after which many states will likely model their own laws, we introduce our discussion of US law with an exploration of BIPA.

The Illinois BIPA

Enacted in 2008, BIPA establishes a regulatory framework for the private collection, use, retention, destruction and disclosure of Illinois citizens' biometric information and identifiers. As noted, BIPA also provides private right of action to such persons "aggrieved by a violation" of the statute. BIPA sat relatively dormant for several years following its enactment, but in each of the last few years, hundreds of complaints have been filed against companies of all sizes and across a range of industries.

The proliferation of BIPA lawsuits is no surprise, as the statute's private right of action includes an exceptionally rich incentive: liquidated damages of $1,000 per negligent violation ($5,000 per intentional or reckless violation), plus recovery of fees and costs, including legal and expert expenses, and no cap on damages. In the class action setting, where potential class members can number in the hundreds or even thousands, potential damages for BIPA cases can be astronomical.

BIPA class actions arise from the use of numerous forms of biometric technology. In some complaints, plaintiffs allege that they were aware of the collection of their biometric data, but they did not consent or were not given notice as required by the statute (e.g., employers collecting fingerprints through timekeeping software or customers submitting facial scans to purchase eyeglasses without the requisite form of notice). In others, plaintiffs allege that they were not aware – nor could they have known – that their biometric data was being collected (e.g., data-scraping of internet photos without the knowledge of the subject or the capture of children's images without consent).

Who – and what – is covered by BIPA?

BIPA regulates private (nongovernmental) entities that collect, store, use or profit from biometric data belonging to Illinois residents. Some private entities, however, are exempt, including financial institutions or affiliates, subject to the privacy notice provisions of the Gramm-Leach-Bliley Act of 1999 (GLBA).

BIPA protects "biometric identifiers" and "biometric information." Biometric identifiers include "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." Biometric information, in turn, is defined as "any information" based on a biometric identifier that can be used to identify an individual. According to one court, "whatever a private entity does in manipulating a biometric identifier into a piece of information, the resulting information is still covered by [BIPA] if that information can be used to identify the person," even if the resulting information is a "mathematical representation or, even simpler, a unique number assigned to a person's biometric identifier."

BIPA does not protect things like writing samples, demographic information, physical descriptions and biological materials covered by the Genetic Information Privacy Act (GIPA). Courts have already interpreted the bounds of some of these exemptions. For example, photographs are excluded from the definition of a biometric identifier under BIPA, and the definition of biometric information explicitly states that it does not include information derived from items excluded under the definition of biometric identifiers. Nonetheless, a number of class action lawsuits have arisen from allegations that individuals' biometric identifiers were gathered from photographs uploaded to the defendants' websites. Some courts have held that a scanned photograph can be subject to the requirements of BIPA in certain circumstances.

Another notable BIPA exemption for biometric data "captured from a patient in a health care setting" or "collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act" (HIPAA) has been subjected to fact-intensive interpretations, with varying results.

What does BIPA require?

BIPA imposes five general requirements on nonexempt private entities that use biometric data in one form or another.

Consent: collection, use, storage	The majority of BIPA lawsuits thus far have alleged violations of Section 15(b), which imposes written consent requirements on private entities that "collect, capture, purchase, receive through trade, or otherwise obtain" an individual's biometric data. The obtaining entity must explain why and for how long the biometric data is being collected, stored or used, and the individual (or that person's legally authorized representative) must execute a written release.
Consent: disclosure and dissemination	BIPA includes a separate consent requirement for private entities that intend to disclose an individual's biometric data. Entities responding to warrants or subpoenas are not bound by this requirement, and neither are entities using the biometric data to complete a financial transaction by the individual. The consent requirements can be satisfied in the employment context by obtaining a written release as a condition of employment.
Prohibition against profiting	BIPA explicitly prohibits private entities from selling, leasing, trading or "otherwise profit[ing] from" an individual's biometric data. This has not generally been the subject of BIPA class actions to date, thus raising a question as to how broadly courts may ultimately interpret the phrase "otherwise profit."
Retention policy	Companies subject to BIPA must also develop, publish and abide by a retention schedule for biometric data they collect. Biometric data must be destroyed by the earlier of the time at which the purpose of the initial collection has been satisfied or three years from the last interaction between the entity and the individual. Over the last two years, there has been an increase in the number of class action lawsuits alleging violations of this requirement.
Reasonable standard of care	Finally, entities possessing biometric data governed by BIPA must "store, transmit, and protect" biometric data (1) using the reasonable standard of care in the entity's industry, and (2) in a manner consistent with how the entity handles other sensitive information. This two-prong requirement underscores the need for companies to incorporate biometrics into their data compliance programs and to stay abreast of both security threats and breach prevention and response best practices.

Biometric protections in other states and municipalities

Over the last few years, a number of states have adopted stand-alone biometrics laws as well as broader privacy laws with biometrics components.

California

The California Consumer Privacy Act (CCPA) imposes stringent notice, consent and retention obligations for consumer and employee "personal information" obtained by companies doing business in the state. The definition of personal information under the CCPA is broad and includes, of course, biometric information.

The definition of biometric information is more expansive under the CCPA than under other laws and includes behavioral information such as "keystroke patterns or rhythms." The CCPA originally applied to employers' collection of applicants' and employees' biometric information as well but granted employers an extended period to comply with the law. The CCPA is enforceable by the California Attorney General, but it does provide for a limited private right of action available to consumers in the event of a breach or disclosure of their personal information resulting from a company's failure to maintain reasonable security procedures.

A year after the CCPA was passed, California voters enacted the California Privacy Rights Act (CPRA), which expanded consumers' privacy protections and rights under the CCPA. The CPRA also enhanced the private rights of action available under the CCPA and created the California Privacy Protection Agency (CalPPA), which will take over enforcement of the CPRA beginning in 2023. Finally, the CPRA further extended the time for employers to comply with the CCPA until 2023.

Colorado

Colorado's Privacy Act expands its consumer protection statute, the Colorado Consumer Protection Act (CoCPA), to regulate commercial entities that process or control personal information of Colorado residents or conduct business in Colorado. The CoCPA defines "biometric data" as "unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account."

The Privacy Act provides consumers with individual rights, such as the right to opt out of the processing of their personal data by companies subject to the law and the right to access, correct, delete or obtain a copy of this data. It further provides enhanced protection of "sensitive" personal data, such as biometric and genetic data. In addition, the act, which resembles the CCPA and the CPRA in many respects, imposes several duties on entities subject to the law, like the duty of care and obligations relating to consumer privacy notices and disclosures. The statute exempts employee and business-to-business data from these obligations, and it does not provide a private right of action.

Maryland

Maryland requires companies to obtain consent prior to collecting facial recognition scans of job candidates during the interview process. The law specifically prohibits potential employers from using a "facial recognition service" to create an interviewee's facial template without prior consent. Facial template is defined as "the machine-interpretable pattern of facial features that is extracted from one or more images of an individual by a facial recognition service."

Separately, the city of Baltimore has prohibited all local government and private entities, including businesses, from using, obtaining, retaining or accessing a facial surveillance technology system in the city until at least December 2022. The ordinance does not prohibit the use of facial recognition technology used in biometric systems designed for security and access control, nor does it prohibit the city police's use of a state imaging system used in criminal investigations. Violations are subject to hefty penalties of up to $1,000 per day as well as the possibility of jail time.

New York City, New York

In 2021, New York City enacted a new regulation addressing, among other things, the collection and use of "biometric identifier information," which the regulation defines as a "physiological or biological characteristic … used by or on behalf of a commercial establishment … to identify, or assist in identifying, an individual." The regulation gives non-exhaustive examples, including eye scans, fingerprints, voiceprints or scans of hand or face geometry, all of which are common forms of biometrics. The regulation imposes a notice obligation and a prohibition on sale.

The notice requirement applies only to commercial establishments (except for financial institutions) that collect, store, convert, retain or share biometric identifier information from consumers. Entities subject to this requirement must place "clear and conspicuous" signage near all customer entrances informing customers in "plain, simple language" that the establishment is collecting, storing, converting, retaining and/or sharing biometric identifier information.

As to the prohibition, the regulation makes it unlawful to "sell, lease, trade, [or] share in exchange for anything of value" biometric identifier information or otherwise profit from a transaction of such information. This appears to be a blanket restriction, which would impact the multilevel chain of transactions between commercial establishments and their corporate parents, affiliates or vendors involved in the data capture and analysis. This regulation also allows for private causes of action under either prong that can be brought by any aggrieved individual whose biometric identifier information is collected in the city, regardless of their state (or country) of residence and regardless of where their data is analyzed, stored or used. The regulation also comes with stiff statutory damages, ranging from $500 to $5,000 per violation.

The regulation adds a local layer to New York's statewide moratorium on the use of biometric identifying technology, which prohibits the use of the technology in state schools until July 2022.

Portland, Oregon

Portland, Oregon's municipal code also prohibits the use of facial recognition technology, but its ban applies only to private businesses operating "public accommodations" (i.e., businesses providing public lodging, amusement, transportation and similar facilities). The ordinance, however, exempts private homes, institutions and other "distinctly private" locales, as well as certain facial recognition technologies used as access controls to certain electronic devices (like iPhones) and social media applications (like SnapChat filters) from the ban. Like New York City, the Portland ban offers a private cause of action for damages sustained as a result of a violation or $1,000 per day of violation, whichever is greater.

Tennessee

Tennessee requires state agencies and educational institutions to obtain consent from students (or parental consent for minor students) before collecting students' "biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking."

In addition, Tennessee expressly criminalizes the theft of biometric data, "such as fingerprint, voice print, retina or iris image, or other unique physical representation," as identity theft. The law states that obtaining or transferring information pursuant to HIPAA or the GLBA is not unlawful.

Texas

In 2009, Texas enacted its own biometric privacy statute governing the "capture and use of biometric identifiers." The Texas statute covers "biometric identifiers," which are limited to retina or iris scans, fingerprints, voiceprints, or the record of hand or face geometry. Exempt from the statute are voiceprints collected by a financial institution. Under this statute, prior to the collection of a biometric identifier for undefined "commercial purposes," the collecting party must obtain informed consent from the individual. Once a biometric identifier is collected, the collecting party may not sell, lease or otherwise disclose the information except in limited circumstances, such as to complete a financial transaction at the request of the owner or if the information is needed to respond to a warrant. Unlike BIPA, Texas's law does not require a written release.

Similar to BIPA, the Texas statute imposes a standard of reasonable care on the party storing or transmitting biometric data that is equivalent to how that party would handle other confidential information. Further, the collecting party must destroy biometric data within a reasonable time or within one year of the date when the purpose for the collection ends. The Texas statute includes a civil penalty of up to $25,000 per violation but is enforceable only by the Texas Attorney General.

Virginia

In 2023, Virginia's Consumer Data Privacy Law will take effect. The bill will apply to certain persons who conduct business in Virginia and control or process at least 100,000 consumers' personal data, or earn over half of their gross revenue from the sale of personal data in addition to processing and controlling personal data of at least

25,000 consumers. Personal data, of course, will include biometric data "generated by automatic measurements of an individual's biological characteristics" but will not include "physical or digital" photographs, video or audio recordings, or "information collected, used, or stored" for certain purposes under HIPAA.

Like Colorado and California, Virginia's legislation will create rights for consumers to access, correct, delete and obtain a copy of personal data, as well as to opt out of processing of their data for specified purposes. The Attorney General will have exclusive authority to enforce the law and will create a dedicated Consumer Privacy Fund for this purpose. With the privacy provisions scheduled to take effect in 2023, the Joint Commission on Technology and Science established a work group to review the bill. The group published its report in November 2021.

Washington

Washington's biometric identifiers law, enacted in 2017, prohibits businesses from "enroll[ing] a biometric identifier in a database for a commercial purpose without obtaining consent, providing notice, and ensuring that the biometric identifier will not be used for a commercial purpose in the future." "Biometric identifiers" under this statute are data "generated by automatic measurements of an individual's biological characteristics," including voiceprint, fingerprint and other "unique biological patterns," but not data generated from photographs or videos.

A "commercial purpose" is defined as a purpose "in furtherance of the sale, lease, or distribution of biometric data to third parties for the marketing of goods and services which are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier." The notice requirement is satisfied if it is made reasonably available to the affected individuals. Notice and consent are "context-dependent." Further, the collecting party may not sell, lease or otherwise disclose a biometric identifier without the individual's consent, subject to some exceptions, which include completing a transaction at the request of the individual or complying with a court order. Businesses may not maintain biometric identifiers longer than reasonably necessary.

Washington's statute does not cover noncommercial uses of biometrics. For example, it expressly exempts from its requirements businesses' collection of data for "security or law enforcement," which is defined as "preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value." Washington's statute does not apply to financial institutions covered by the GLBA or to activities covered by HIPAA and does not provide for a private right of action. The Washington Attorney General's office has the power to enforce the statute pursuant to Washington's Unfair Business Practices Consumer Protection Act.

Biometrics in state data breach laws

Many states address biometrics through their data breach notification laws. Although each state varies in the specifics, the laws typically apply to businesses that operate within the state and collect personal information from resident consumers. The laws generally provide that entities that possess the personal information must protect that information from unauthorized access and notify affected consumers if their information is compromised. Some statutes apply only to commercial entities, while others apply to nonprofit entities or natural persons as well. Most of the states provide that persons who comply with HIPAA or the GLBA are in compliance with or are exempt from the state law.

Other federal and state activity

There are a few sector-specific federal laws that include biometric information in their protections as well as industry-specific guidance. In 2012, the FTC issued a staff report titled "Best Practices for Common Use of Facial Recognition Technologies." Although companies are not bound by these best practices, the FTC has, on occasion, exercised its authority under Section 5 of the FTC Act to investigate privacy-related issues, including those arising from facial recognition technology. Further, FTC complaints have been filed against companies in the IoT and AI sectors, alleging that the companies were engaging in deceptive acts or practices in or affecting commerce.

For example, in 2021, the FTC commenced enforcement proceedings against a company that allegedly deceived consumers about its use of facial recognition technology and its retention of consumers' biometric data. The company offered a free app that allowed consumers to upload photos and videos to the company's servers for storage and organization. The app later launched a facial recognition feature that enabled users to tag people and group together uploaded content accordingly.

The FTC alleged that the defendant violated Section 5 of the FTC Act by misrepresenting what happened to users' content after it had been uploaded. According to the FTC, the company gave the impression that it was not running facial recognition algorithms unless the customer opted in to the feature but, in fact, did enable the feature for most users and without providing the option to disable the feature. The company also allegedly used data gathered by the AI-powered technology to develop a stand alone facial recognition service for sale to its enterprise customers. Significantly, the only users exempt from this challenged practice were residents of Illinois, Washington and Texas (the only states with specific biometrics laws at the time) and of the European Union (which is subject to the General Data Protection Regulation (GDPR)). The FTC further alleged that the company falsely stated that it deleted users' content when they deactivated their accounts, when the company's practice was to retain the content indefinitely.

The FTC complaint resulted in a consent order that required the company to engage in several remedial actions, including deleting content and destroying facial recognition tools developed using the data collected without consent. Of particular note is that the consent order adopted a very broad definition of biometric information.

At the state level, the Vermont Attorney General sought an injunction against Clearview AI arising from that company's alleged practice of collecting images of Vermont residents and using AI to create "maps" (i.e., templates) of their faces without their knowledge or consent. The complaint, filed in March 2020, alleged violations of the Vermont Consumer Protection Law and its Fraudulent Acquisition of Data Law.

What looms on the horizon?

Federal privacy laws have been proposed in the US Congress, including legislation that would specifically address the commercial use of facial recognition technology and other biometrics. To date, none of these proposed laws has gained traction, leaving the federal government well behind many states on consumer privacy legislation. There have also been sporadic calls for other forms of federal government regulation, such as the creation of an overarching federal agency modeled after the Food and Drug Administration to govern facial recognition technology.

It is only a matter of time before more states and cities join Illinois, Texas and Washington in strictly regulating the collection, use and storage of biometric information, as several states have recently considered similar statutes. It is also possible that state Attorneys General will scrutinize the area more closely.

The continued widespread adoption of, and novel uses for, biometric technology will likely also give rise to more traditional claims and theories of liability. For example, some plaintiffs' attorneys are already attempting to leverage existing unfair and deceptive practice laws to pursue claims where laws like the Illinois BIPA do not apply. In late 2021, a putative class action was filed in New York federal court against an insurer that allegedly collected, stored, analyzed and used members' biometric data without their consent.

Among other things, the plaintiff alleged that the insurer requires insureds submitting a claim to upload a video of themselves narrating the circumstances of the loss and that the company admitted in a series of tweets that it applies AI facial recognition to the videos to analyze the claims for fraud. The plaintiff also alleged that the insurer expressly and impliedly promises to its insureds (through its data privacy policy) that it will not collect, require, sell or share consumers' biometric data in the context of consumers' use of the insurer's products and services. These practices, according to the plaintiff, helped the insurer's bottom line by lowering loss ratios and operating costs. The plaintiff's complaint sought damages and injunctive relief under novel theories of statutory and common law, including violations of New York State's Uniform Deceptive Trade Practices Act as well as breach of contract and unjust enrichment. Such claims could become more common in the future, in New York and elsewhere.

Unforeseen implications?

Finally, the collection of biometric data from employees may have unforeseen implications beyond statutory law. In a possible sign of things to come, in September 2019, a union filed a complaint against the Metro-North Commuter Railroad Company (MNCR), which runs the New York City subway and regional commuter trains, seeking injunctive relief to prevent the MNCR from requiring its employees to use a new fingerprinting system to log in and out of work. Specifically, the union sought to enjoin the MNCR from implementing its biometric fingerprint-scanning system. The crux of the dispute arose from a 2010 New York State Labor Department opinion that stated that only voluntary fingerprinting of employees is permissible. On the one hand, the MNCR wanted to implement an efficient timekeeping system that would, in part, curtail overtime cheating. On the other

hand, the employees did not want their fingerprints to be used for other purposes, such as criminal background checks. These underlying and conflicting interests are typical in the context of implementing biometrics systems in the workplace.

Additional litigation or regulatory risk may arise from allegations that facial recognition technology has enabled or masked discrimination against classes of people protected by federal laws based on personal characteristics such as age, sex, race or disability. For example, if a company were to use biometric data collected for one purpose in making determinations that subject such protected persons to discriminatory practices, that company could face a federal class action lawsuit. As a related issue, improper use of facial recognition technology could give rise to a host of constitutional concerns. This risk highlights what was discussed earlier, vis-à-vis both bias and mission creep.

Related Attorneys

Frank Nolan
Partner, Biometrics Guide Editor
New York

Jessica Rodgers
Associate
Washington DC

Michael Bahar
Partner, Co-Lead of Global Cybersecurity & Data Privacy
Washington DC

Brandi Taylor
Partner
San Diego

MJ Wilson-Bilik
Partner
Washington DC

Melanie Ramey
Associate
Atlanta

United Kingdom and European Union

by Gayle McFarlane, Philip James, Marie McGinley, Olaf Van Haperan, Nils Müller, Emmanuel Ronco

Gayle is a Partner in the Birmingham office, Philip is a Partner in the London office, Marie is a Partner in the Dublin office, Olaf is a Partner in the Rotterdam office, Nils is a Partner in the Munich office and Emmanuel is a Partner in the Paris office.

The General Data Protection Regulation

The GDPR came into force while the UK was part of the EU, and little has changed with regards to biometric data in the UK since then (other than the occurrence of Brexit, which has now resulted in the splitting of GDPR into EU GDPR and "UK GDPR" – which is the EU GDPR as implemented in the UK); therefore, unless otherwise stated, for the purposes of this paper, references to the GDPR will also include the UK GDPR. In addition, personal data in the UK is regulated by the UK Data Protection Act, and any information that is placed or accessed on a device that is not personal data but that may be used in connection with biometric-related applications is regulated by PECR (the Privacy and Electronic Communications Regulations).

The concept of personal data has for many years been wide enough to encompass many forms of biometric data, at least while that data has been at an individual level. However, in 2016, recognizing the development of this technology, the GDPR introduced an official definition of biometric data, meaning:

"personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data"

If biometric data meets this definition, then where it is used for the purpose of uniquely identifying a natural person, it constitutes "special category data" under the GDPR, meaning that the purposes for which it can be processed are seriously limited, and the standard of security to which it must be subject is enhanced.

Who – and what – is covered by the GDPR?

The GDPR regulates any legal person (individual or corporate) who processes (which includes any operation you could contemplate applying to personal data, such as collection, storage, use or even destruction of) personal data, including biometric data, and who is established in the EU or the UK, is subject to the GDPR through the application of public international laws, or is not established in the EU or the UK but whose processing of personal data relates to:

- offering goods or services to individuals in the EU or UK (respectively);
- monitoring the behavior of individuals in the EU or UK (respectively).

It does not apply to individuals processing personal data in a purely domestic context.

Where a person legally determines the manner in which and the purposes for which the biometric data is processed, they are referred to as the "controller" of this data, the term we will use in this section of the guide. In most cases, this will be the organization rolling out the biometric technology, e.g., the organization that introduces fingerprint-based access controls. However, as the technology becomes more sophisticated, and the technology provider starts to either determine the purposes for which the data is used or to use the data independently, for example, to inform its own machine learning or AI algorithms, the provider may also be a controller. This is becoming a more and more complex analysis for organizations to undertake.

The definition of biometric data in the GDPR is very wide and potentially captures any information about a person's physical or behavioral attributes, but there are two important caveats:

- it must be used to identify them; and
- it must result from specific technical processing.

This means, for example, that while a photograph could arguably be biometric data in and of itself, it is not considered to be biometric data under the GDPR unless it is being used in the context of (for example) facial recognition technologies.

Unlike the Illinois BIPA statute discussed in the US section of the guide, the GDPR protects individuals against the unauthorized processing of information about them, including writing samples, demographic information, physical information and biological materials, where those items result from technical processing and are used to identify them.

What obligations do controllers have under the GDPR with regards to biometric data?

Transparency

Controllers are required to process personal data lawfully and, in particular, to ensure that they have given sufficient transparency information so that individuals are able to assess for themselves the impact of allowing their personal data to be processed.

There is a lot of information mandated to be provided, but of particular relevance to users of biometric technologies, a controller must identify itself, the purposes of the processing (and information about the corresponding lawful basis – see below under "Purpose limitation and lawfulness" for further information) and who else the controller might share the data with (and if that might take their data to jurisdictions where equivalent protection for their data is not provided). Individuals must also be informed of how long the biometric data will be stored and the rights that they have in relation to that data.

Purpose limitation and lawfulness

Biometric data should only be collected for "specified, explicit and legitimate purposes," as set out in the transparency notices provided to individuals, and the processing should not be extended to any processing that is incompatible for those purposes.

However, in order to be legitimate, the purpose for processing must be one that is set out as a "lawful basis" for that processing under the GDPR.

The most commonly used lawful bases in this context are where the processing is necessary for:

- on the basis of consent for the specified purpose, which must be freely given specific, informed and unambiguous indication of the data subject's wishes;
- the performance of a contract with the data subject;
- compliance with a legal obligation of the controller;
- the performance of a task carried out in the public interest (which must be laid down in law); or
- the purposes of the legitimate interests pursued by the controller or by a third party – but in this case:
  - » the controller must inform the individual of the nature of the legitimate interest; and
  - » balance the legitimate interests against the interests or rights of the individual – if those interests or rights override the legitimate interest (e.g., it is a disproportionate invasion of privacy when looked at in light of the objective to be achieved), legitimate interest cannot be relied upon.

"Necessity" is a strict test: the processing must be objectively necessary to meet the purpose of processing, and this is a matter of fact. Processing that is useful or necessary as part of the controller's business purposes but not objectively necessary for the purpose will not be sufficient.

In addition, because biometric data used for the purposes of identification is classified as "special category data," an additional lawful basis for processing must be found from an even more restricted list. In most cases, biometric data can only be processed for identification purposes where the processing is:

- on the basis of explicit consent;
- necessary for the controller's employment or social security obligations (where laid down in law); and
- necessary for reasons of substantial public interest (where laid down in law).

This second requirement for a lawful basis provides controllers with the most problems, unless the relevant member state has made a particular regulation for the use of biometric data, which most have not. Where the use of biometric data is for common activities, such as time and attendance or security, controllers must demonstrate that it is necessary for the purposes of a legal obligation already set down. Due to many jurisdiction's legislatures not having specifically legislated in this area, controllers tend to be left with only one option – to rely upon consent.

The issue of consent

Due to the very limited circumstances in which biometric data is permitted to be processed, many consumer products rely on the basis of consent to use facial or fingerprint recognition on electronic devices or other services. This is possible where the use of personal data is integral to consumers having a clear choice as to whether to use the service or not.

However, in the EU and UK data protection regimes, consent is held to a higher standard than might be encountered in other jurisdictions, including the US. Due to the requirement that consent is "freely given," it is almost impossible to rely on the lawful basis of consent in an employment relationship, due to the disparity of power between an employee and employer. Employers wishing to go down this route would need to take great care that employees were genuinely given an opportunity to positively elect to use the biometric system (rather than allowing an opt-out), and that there was no potential implication of any pressure or adverse impact on the employee for not providing consent. In addition, in order to comply with transparency requirements, sufficient information must be provided regarding the nature of the processing.

Data minimization and accuracy

Controllers must ensure that the data processed is "adequate, relevant and limited to what is necessary." The GDPR prohibits data being collected "just in case," which is a challenge in the context of any "big data" analysis. Processing must also ensure that data is accurate and, where necessary, kept up to date, and that inaccurate data is corrected or erased without delay. Again, this is an area where it may be difficult for organizations to comply.

Security and storage limitation

Biometric data should not be kept in an identifiable format for any longer than is necessary to achieve the purpose for which it was processed. As special category data, it also attracts a higher requirement in relation to security precautions, and controllers must put in place all appropriate protections for the data.

Data protection by design and by default and impact assessments

Controllers must always, in the implementation of new technologies, ensure that they implement appropriate technical and organizational measures designed to implement the data protection principles, and ensure that, by default, only personal data that is necessary is processed. In the context of biometric data, controllers may also need to carry out a data protection impact assessment (DPIA) to consider the impact of processing on individuals. If, following that impact assessment, there is still a high risk to the rights and freedoms of individuals, then processing cannot proceed within the authorization of the supervisory authority. As part of any DPIA, a regulator will always be looking to see if another means or method could have been used (i.e., other than biometrics) to achieve the same goal. This is a consistently difficult criterion to satisfy, as it is often hard to justify. In new technologies, however, such as in open banking and payments, technical standards set out what methods may be used to verify and authenticate digital IDs, and when these are statutory or required by a regulator, this can aid justification. Industry codes and regulations must also be reviewed and complied with (in addition to data protection and GDPR).

Rights of individuals

Individuals have the right to:

- access any of their personal data, as well as information relating to its processing;
- restrict the processing of that data, for example, where its accuracy is contested or the processing is unlawful;
- object to the processing when it is on the basis of "legitimate interests";
- withdraw consent to the processing when it is on the basis of consent;
- erasure of their personal data when it is no longer required, or they have withdrawn consent or objected to processing; and
- have incorrect or incomplete personal data rectified or completed.

Requests to exercise these rights should be complied with within one month, and there are only very limited exceptions. Where automated decision-making or profiling is used, the individual may be entitled to an explanation of how that decision was reached, including the logic of that decision (which can be very complex if AI is used), and have the right to obtain human intervention, express their point of view and challenge the decision.

This can cause substantial difficulties for controllers using biometric data to manage, particularly where data about one individual is mixed with data about other individuals (for example, in relation to closed-circuit television (CCTV) images), and is a cost that controllers must consider when contemplating the use of biometrics.

Rights of action

The GDPR grants any person "who has suffered material or non-material damage as a result of an infringement … the right to receive compensation from the controller or processor for the damage suffered."

This seems to be a very wide right, which, combined with the ability for individuals to be represented by a representative organization, could give rise to a significant risk of class actions for misuse of biometric data. These, however, are yet to materialize. That does not mean that claims have not been made, and a selection of relevant cases are included below.

Unlike regimes in the US, there is no specified damages regime, and, therefore, the claimants would need to demonstrate their loss. Although the GDPR anticipates that such losses may be material or nonmaterial, how these are quantified is still an area to be settled if more cases are produced.

Regulatory action

In addition, in a case of a breach of the GDPR, the data protection supervisory authorities have the ability to take action against controllers, imposing fines of up to 4% of annual worldwide turnover or €20 million/£17.5 million (whichever is the greater), depending on the nature of the breach.

Examples of claims and enforcement action in the UK and EU member states

Finland

In September 2021, the Finnish Data Privacy Act (DPA) found that the Finnish police had unlawfully relied on the facial recognition software Clearview AI in 2020. It ordered the Finnish police to bring processing into compliance with the GDPR and to notify identifiable data subjects of this breach.

France

In February 2020, the Administrative Tribunal of Marseille annulled a facial recognition system experimentation launched in two high schools because teenagers' biometric data were processed without any legal basis, as consent was not freely given.

Germany

In June 2020, the Berlin-Brandenburg Regional Court for Labor Law held that an employer could not rely on the lawful basis of carrying out its obligations in relation to employment to install a time-tracking system that uses the fingerprints of employees.

Iceland

In August 2020, the Icelandic supervisory authority held that an employer did not lawfully process the fingerprint data of its employees for the purpose of logging in and out the employees in the company's payroll system.

Ireland

In November 2020, the Irish Data Protection Commission (DPC) made a preliminary finding in respect of a complaint from a prison officer that a security system used in Irish prisons was in breach of the GDPR. The security system involved scanning prison officers' thumbprints in an automated vending system to provide appropriate access to security keys used within the prison. A key aspect of the complaint was that there was no appropriate legal basis in place for the processing of biometric data. The DPC investigated the matter and concluded in its subsequent report that "the Irish Prison Service had not established a legal basis for the processing of biometric data at issue in this case under Articles 6 and 9 GDPR and/or sections 46 and 49 of the Data Protection Acts 1988 to 2018" and that, as a consequence, "the processing of the relevant biometric data of the Complainant in connection with the set-up and operation of the relevant key vending system in Castlerea Prison is unlawful." A decision was made to bring an appeal on certain aspects of the findings of this investigation to the High Court of Ireland.

Following media reports in February 2020 regarding a facial recognition trial for attendance monitoring purposes in a secondary school, the DPC met with members of staff and the Board of Management of the school. The DPC outlined the data protection issues surrounding the use of biometrics data, specifically facial recognition technology, in an educational environment, including processing the data of minors. Following the meeting, the school provided the DPC with a full written report on the matter, including confirmation that it did not proceed to trial the attendance monitoring product in question. In Ireland, the DPC regularly conducts inspections of schools where reports of biometric attendance systems or trials are received. The DPC considers that exposure to intrusive methods of surveillance without sufficient legal basis or justification can desensitize students at a young age to such technology and lead to their ceding their data protection rights in other contexts too.

Italy

In January 2021, the Italian supervisory authority imposed a fine of €30,000 on (and ordered the deletion of data by) a local public health body for using an attendance detection system based on biometric data of employees, as it was relying on consent, which was not valid, and had not adequately informed employees of the processing.

In September 2021, the Italian supervisory authority fined the Commercial University of Milan €200,000 for using noncompliant supervisory systems as part of its provision of remote exams to students during the COVID-19 pandemic on the basis of consent, which was not freely given.

Netherlands

In December 2020, the Dutch supervisory authority imposed a formal warning on a supermarket that used facial recognition to scan visitors' facial images, register them and compare them with a facial image database of individuals who were banned from the supermarket in order to protect staff and customers. The supervisory authority confirmed that consent was not given by simply entering the supermarket and seeing a sign and that no other compelling public interest applied to make this processing lawful.

In April 2020, the Dutch supervisory authority also imposed a €725,000 fine on an organization that used fingerprint scanners for employee attendance and time registration, ostensibly on the basis of consent. However, the consent was invalid due to the imbalance of power in an employer/employee relationship and the fact that the choice of biometric controls was not proportionate, as the objective could be achieved by less intrusive means.

In December 2019, a Dutch court prohibited a shoe retailer from using employee fingerprints to log on to the cash register system, because it did not consider this necessary for authentication or security purposes.

Lithuania

In June 2021, the Lithuanian DPA fined a sports club approximately €20,000 for processing the biometric data of its customers and employees in violation of the GDPR, in particular, because the club relied on consent as the lawful basis, which was not freely given, as it was not voluntary.

Poland

In February 2020, the Polish supervisory authority imposed a fine of €4,700 (PLN 20,000) on a primary school for unlawful processing of children's biometric data by requiring the use of a fingerprint scanner to check payment when using the school canteen. The processing was considered disproportionate. This was later overturned in court.

Spain

In October 2021, the Spanish supervisory authority fined a controller €20,000 (reduced to €16,000) for implementing a biometric identification system to control worker access without carrying out a DPIA beforehand, following a complaint brought by a trade union.

In July 2021, the Spanish supervisory authority fined a supermarket chain €3,150,000 (reduced to €2,520,000) in relation to its video surveillance system, which used biometric data to identify individuals who had previously committed crimes at its store and who were banned from entering.

In May 2021, the Spanish supervisory authority warned a regional Department for Public Education and Universities for not adequately informing its workers about a biometric identification system that was in the process of being implemented.

In February 2021, the Spanish supervisory authority imposed a warning sanction on a local council for using a biometric control system to monitor the working hours of employees without having informed them in accordance with Article 13 GDPR.

In March 2020, the Catalan DPA issued a warning to a public school for using biometric data to monitor student attendance.

In April 2019, the Spanish supervisory authority issued a warning to an airline for not providing sufficient transparency information to workers regarding a fingerprint clock-in system.

Sweden

In March 2021, the Court of Appeal in Stockholm upheld a decision of the Swedish DPA (IMY) to fine a school €20,000 (SEK 200,000) for using facial recognition technology to register student attendance, as consent could not be freely given.

In February 2021, the Swedish supervisory authority fined the Swedish Police Authority €248,218 for unlawful use of a facial recognition app in breach of the Swedish Criminal Data Act.

United Kingdom

In November 2021, the UK Information Commissioner's Office (ICO) issued a provisional intent to issue a monetary penalty of more than £17 million relating to the use of biometric data and facial recognition by an AI provider, following a joint investigation with the Australian Information Commissioner.

In May 2019, the UK ICO issued an enforcement notice against Her Majesty's Revenue and Customs (HMRC) in relation to their collection of voice ID records without adequate consent, requiring deletion of records and a change to processes going forward.

Specific derogations in the UK and EU member states

The GDPR allowed for individual member states (including the UK) to make additional, specific rules about the use of biometric data. Very few member states took the opportunity, which has led to some clear areas where practice and legislation do not align. However, examples include:

France

Employers may process biometric data that is strictly necessary to control access to workplaces and to equipment/devices and applications used by the employees, provided it is in accordance with the French supervisory authority's model regulation on the processing of biometric data in the workplace (dated January 10, 2019), and a DPIA has been carried out. Employers will need to be able to justify why the workplace, equipment or application requires such a high level of security protection; demonstrate why other, less intrusive, means of security would not be sufficient; and must still comply with their security and transparency obligations, as well as justifying and documenting the choices they make in selecting and configuring the technologies.

Germany

Controllers can also process biometric data on the basis of Sec. 22 (1) Federal Data Protection Act, for example, where the processing is urgently necessary for reasons of substantial public interest. In the employment context, controllers can rely on Sec. 26 (3) and (4) Federal Data Protection Act, which include works council agreements as a legal basis (where a works council exists). In both cases, controllers must take appropriate technical and organizational measures to safeguard the interests of individuals in accordance with Sec. 22 (2) Federal Data Protection Act. These measures may include in particular the designation of a data protection officer or the encryption of personal data.

Italy

Biometric data must be processed in accordance with the additional safeguard measures issued by the Italian supervisory authority (the Garante) every two years.

Netherlands

Article 29 of the Dutch Implementation Act provides an exemption to the prohibition on processing biometric data where the processing is necessary for authentication or security purposes. This exemption is likely to be narrowed following a public consultation for a new "Data Protection Collective Act" to restrict processing further to the extent necessary to achieve a compelling interest of lawful access to certain places, buildings, services, products, information systems or work process systems. This "compelling interest" is an interest that must go beyond regular business or organizational interests (such as efficiency or cost savings) and might include protection of public health, prevention of environmental damage or safeguarding vital processes – the example given in the consultation is in relation to the security of a nuclear power plant.

Poland

The Polish Labor Code (Act of June 26, 1974, as amended) restricts when an employer may process an employee's biometric data where it is necessary in order to control access to particularly important information, the disclosure of which may expose the employer to damage, or access to premises requiring special protection.

Portugal

Law no. 58/2019 of August 8, 2019, contains specific requirements in relation to the processing of data relating to employment relationships, including in relation to video surveillance systems and biometric data. Article 28(6) limits employers to only processing biometric data for the purposes of attendance and access controls; only a representation of the biometric data can be used, and it should not be possible to reconstitute the original biometric data.

United Kingdom

The Protection of Freedoms Act 2012 further regulates the processing of biometric information about children in schools by relevant authorities, requiring that authorities notify and obtain consent from parents but also that they respect any withdrawal of that consent by the child.

Related Attorneys

Gayle McFarlane
Partner
United Kingdom

Philip James
Partner
United Kingdom

Marie McGinley
Partner
Ireland

Olaf Van Haperen
Partner
Netherlands

Nils Müller
Partner
Germany

Emmanuel Ronco
Partner
France

Robbert Santifort
Senior Associate
Netherlands

Mélanie Dubreuil-Blanchard
Associate
France

Constantin Herfurth
Associate
Germany

Leona Chow
Solicitor
Ireland

Sophie Delaney
Solicitor
Ireland

Asia

by Rhys McWhirter, Hilary Chan and Woody Yim

Rhys is a Partner and Head of Technology and Hilary and Woody are Trainee Solicitors in the Hong Kong office of Eversheds Sutherland (International) LLP.

Hong Kong

Hong Kong has not enacted stand-alone legislation specifically addressing biometric data. Rather, the collection, processing and use of personal data, in general, is governed by the city's key data protection statute, namely the Personal Data (Privacy) Ordinance (**PDPO**), which entails a range of duties and obligations to be discharged by the data user in respect of personal data. Therefore, the key question is whether biometric data is considered to be personal data under the PDPO.

Under the principle-based approach of the PDPO, the statutory body enforcing the legal code has unsurprisingly adopted a more prudent approach in giving tailored recommendations to biometric data users in its guidance note. It is inclined to hold the position that biometric data is regarded as personal data under the PDPO, in particular where it is linked with personal data in a database and is capable of revealing identities. As a result, those who collect or use biometric data should ensure that such data is collected from individuals on a fully informed basis, in the minimal amount and in a fair and transparent manner.

Once collected, the data should be securely processed and only kept for as long as necessary for the purpose of collection. It cannot be used for any new or unrelated purposes or transferred to a third party, except with the individual's express and voluntary consent, or where a certain limited exemption such as crime prevention or news reporting applies. Some personal characteristics that correspond with biometric data, such as DNA and retina images, may contain rich information about a person capable of revealing physical health or even mental conditions. Data users must be prudent in using such corresponding data and ensure that it is not used for another unrelated purpose without consent. Individuals are entitled to exercise their data subject rights, including those to access and make correction to their data. When external contractors are engaged in the handling of biometric data, data users must adopt contractual or other means to guard against prolonged retention periods at the external contractors and to ensure data security.

The city has recently stepped up its legislative efforts to curb doxxing, i.e., the act of publicly revealing previously private personal information about an individual, usually through the internet. It is now a criminal offense to disclose the personal data (including biometric data) of an individual without their consent. The new law even extends the protection to cover the individual's family members and entails a maximum fine of HK$100,000 and imprisonment of up to two years for any unlawful disclosure. The guidance note further recommends that a privacy impact assessment should be carried out to help avoid or minimize any impact on the individuals concerned. In such assessment, we should explore the "least intrusive option" for achieving the collection purpose. In other words, unless the collection of biometric data can be justified by overriding reasons, we should adopt another option that will involve less sensitive and lesser amount of personal data. Attendance taking and security control, for example, are not on their own sufficient reasons for biometric data to be collected.

Corporations that regularly collect and store a vast amount of personal data ought to exercise extra caution when it comes to data security, staff training and periodic audits of the data system, especially as sensitive biometric data is at stake. Any unauthorized or accidental data leakage would possibly lead to grave reputational, if not legal, risks.

People's Republic of China (PRC)

The PRC has certainly upped its game in governing the handling of personal information with the promulgation of the PRC Personal Information Protection Law (**PIPL**) on November 1, 2021, officially consolidating its data privacy legislation with a nationwide regime that has been described to be as strict as, if not stricter than, the EU's GDPR.

As a nation with such prevalent usage of biometric information by its citizens in their daily lives, from taxi-hailing to online shopping, the governance of biometric data is certainly provided for in the PIPL. The definition of "sensitive personal information," which imposes more stringent requirements in addition to the baseline requirements under the PIPL, includes "information on biometric characteristics." In order to process sensitive personal information, personal information handlers would need to obtain the data subject's separate consent. Further guidelines have since been published by the Cyberspace Administration of China, specifying that "separate consent" means consent from the data subject for "each type of processing" envisaged for "each type of personal data" processed, and that bundled consent or general consent clauses cannot be relied upon. In addition, when handling sensitive personal information, personal information handlers should notify data subjects of the necessity of such processing and the impact on their rights and interests for processing the sensitive personal information and conduct an impact assessment in advance of such processing.

This development would be in line with the current position under the Personal Information Security Specifications, which have provided that explicit consent from data subjects would be required to collect their biometric data and provide information about the purpose, method, scope of collection, etc.

In addition, there are industry-specific data privacy regimes that similarly provide for the handling of biometric data, which continue to apply concurrently with the PIPL. One example would be the Personal Financial Information Protection Technical Specifications, which apply to the banking and finance industry, which were clearly introduced and driven by the fast development of new payment solutions based on biometric information (most notably, facial recognition technology) in the PRC. Biometric identification information (e.g., facial recognition, fingerprint recognition) is classified as C3 information, requiring special encryption measures to be undertaken to prevent unauthorized parties from obtaining such information, such as by adopting relevant control measures during any transmissions and prohibiting outsourced service institutions and external cooperation institutions from retaining such information by contract or agreement.

Further, the PRC has included the Biometric Information Protection Requirements within its pipeline of legislations to be promulgated in 2022 to further supplement the PIPL. The draft consultation paper, which was released in 2019, proposes provisions that are largely in line with the PIPL requirements for separate consent, notification and encryption. It further provides that any biometric data collected from a data subject should be stored separately from other personal information collected from the same data subject.

On that note, there is a lot that is yet to be uncovered regarding the PRC data privacy regime for biometric data. The legislative development in the PRC has long adopted a pragmatic "learn from doing" approach, and there will certainly be continued legislative efforts in the future that will further fine-tune the current data privacy regime consolidated under the PIPL. With that, all we can do now is continue to watch this space for continued developments.

Singapore

In Singapore, the Personal Data Protection Act 2012 (No. 26 of 2012) (**PDPA**) provides the baseline standard governing the collection, use and disclosure of individuals' personal data by organizations. The PDPA applies to all organizations and has an extraterritorial effect. With its data protection regime being relatively new as compared to other jurisdictions, it is not surprising that Singapore, similar to Hong Kong, does not yet have clearly defined regulations specifically for the governance of biometric data. The term "biometric data" is not used in the PDPA, and instead, similar to health data, biometric data is considered a type of personal data and, therefore, is covered by the PDPA.

For specific private sector entities such as the banking sector, other statutes apply for the handling of personal data on top of the baseline standard imposed under the PDPA. For example, organizations in the banking sector would be bound by additional legislation in the form of the Banking Act and the Telecommunications Act.

Recently, the city has made an effort to strengthen its data protection regime with the passing of the draft Personal Data Protection (Amendment) Bill (Amendment Bill) in the Singapore Parliament in November 2020. Certain sections of the Amendment Bill have now come into force under the Personal Data Protection (Amendment) Act 2020 (as of February 1, 2021). These include mandatory data breach notification, an expanded deemed consent framework, new exceptions to the express consent requirement and new offenses for the egregious mishandling of personal data or the unauthorized reidentification of anonymized information. The sections on increased financial penalty and the right of data portability were expected to come into force no earlier than February 1, 2022. However, to date, no regime or guidance specific to the governance of handling biometric data has been introduced.

Related Attorneys

Rhys McWhirter
Partner
Hong Kong

Hilary Chan
Trainee Solicitor
Hong Kong

Woody Yim
Trainee Solicitor
Hong Kong

Middle East

by Nasser Khasawneh, Christine Khoury, Anum Saleem, Cristina Craciun and Sarah Khatib

Nasser is a Partner and Christine is a Principal Associate in the Dubai office, Anum is a Principal Associate in the Riyadh office, Cristina is an Associate in the Doha office, and Sarah is a Senior Associate in the Amman office of Eversheds Sutherland (International) LLP.

United Arab Emirates

General overview

Laws in the United Arab Emirates (UAE) can be divided into mainland/onshore UAE laws and laws specific to free-trade zones.[1]

Free-trade zones in the UAE are areas that have a special tax, customs and import regime and are governed by their own framework of regulations (with the exception of "UAE criminal law"). Free zones may be broadly categorized as seaport free zones, airport free zones and mainland free zones. Free-trade zone exemptions are (i) 100% foreign ownership of the enterprise, (ii) 100% import and export tax exemptions, (iii) 100% repatriation of capital and profits, (iv) corporate tax exemptions for up to 50 years, and (v) no personal income taxes.

In line with the UAE's 50th anniversary, 40 new federal laws have been approved. This represents the biggest legislative reform in the history of the UAE. The reforms include the introduction of a federal data protection framework with the approval of Decree-Law No. 45 of 2021 on the Protection of Personal Data (the "Personal Data Protection Law") and Decree-Law No. 44 of 2021 on the Data Protection Office Establishment (the DPO Law).

The Personal Data Protection Law applies to all UAE residents and those working there and to the processing of personal data by controllers or processors inside or outside the UAE. Similar to the data protection laws in the region – most recently, the Saudi Personal Data Protection Law, which came into force on September 24, 2021 – the Personal Data Protection Law does not apply to government data or government entities controlling or processing personal data. This exception diverges from that undertaken by the GDPR.

The Personal Data Protection Law further excludes from its scope personal data held by judicial and security authorities, the data subject processing their data for personal purposes, personal health data, personal banking and credit data, and free-zone companies and institutions subject to relevant data protection legislation.

Biometric data

As it stands now, biometric data are not dealt with under a separate or stand-alone law; therefore, biometric data is treated as any other data protected under several laws, as explained above. Having said that, biometric data are specifically defined under both Dubai International Finance Centre (DIFC) and Abu Dhabi Global Market (ADGM) laws.

Personal Data Protection Law

Both laws, the Personal Data Protection Law and the DPO Law, were issued on September 20, 2021. The Personal Data Protection Law shall take effect January 2, 2022. The Implementing Regulations supplementing it should be issued within six months from the date the Federal Data Protection Law was issued. The DPO Law takes effect on the next day after it was issued.

1 Certain freezones have their own respective data protection legislation, which only applies within the borders of the relevant freezone, such as the Dubai International Financial Center (DIFC), the Abu Dhabi Global Market (ADGM) and the Dubai Healthcare City.

The Personal Data Protection Law provides the following definitions:

Personal data is defined as "any data relating to a specific natural person, or relating to a natural person that can be identified directly or indirectly through the linking between the data, through the use of identification elements such as his name, voice, image, identification number, electronic identifier, geographical location, one or more of his physical, physiological, economic, cultural or social characteristics. This includes sensitive personal data and biometric data."

Sensitive personal data is defined as "any data that directly or indirectly reveals a natural person's family, ethnic origin, political or philosophical opinions, religious beliefs, criminal record, biometric data, or any data relating to that person's health, including physical, psychological, or mental, physical, genetic or sexual status. This includes information related to the provision of health care services to him that reveals his health status."

Biometric data is defined as "personal data resulting from processing using a specific technology related to the data subject's physical, physiological or behavioral characteristics that allow the identification or confirmation of the unique identification of the data subject, such as a facial image or fingerprint data."

The Personal Data Protection Law prohibits the processing of personal data without the data subject's express and unambiguous consent save for certain instances relevant to the protection of the public interest, the public health or the data subject's interests, among other exceptions. Moreover, the procedures to withdraw consent must be as simple as those asking for consent, thereby giving data subjects the freedom and accessibility to withdraw consent at any point and obliging the controller to destroy said data.

Similarly, the data subject can consent to the cross-border transfer of their personal data even if the transferee country does not have an adequate data protection framework. The Personal Data Protection Law places significant emphasis on the consent of data subjects and, thus, it means that data subject consents will become crucial to all processing activities going forward.

DIFC Data Protection Law

The DIFC was launched in accordance with UAE Federal Decree No. 35 of 2004. The DIFC has issued a new data protection law called Data Protection Law 2020 (DIFC DPL).

The DIFC DPL came into force on July 1, 2020, and enforcement began on October 1, 2020. DIFC DPL provides a framework in which personal data may be collected, used, stored and transferred to other jurisdictions outside the DIFC or individuals with similar levels of protection. The DIFC DPL applies to the following: (1) businesses incorporated in the DIFC (irrespective of whether the processing of personal data occurs within the DIFC); and (2) businesses that process personal data in the DIFC as part of stable arrangements, other than on an occasional basis, regardless of their place of incorporation.

This means that it is applicable to both controllers and processors in the DIFC, as well as such entities outside the DIFC in the context of the processing conducted as part of stable arrangements, other than on an occasional basis. While non-DIFC entities may be subject to the law either directly or indirectly, they are not necessarily required to register or provide notification of operations to the commissioner other than by way of the relationship with the DIFC-based relevant entity, nor are they required to complete other administrative tasks.

According to the DIFC DPL, personal data is any data relating to an identified natural person or identifiable natural person. An identifiable natural person is a natural living person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data or an online identifier, or to one or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity.

Special category data is personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership, and health or sex life, including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person. Under this definition, "personal data" is extended to "direct or indirect" data that is sensitive to the data subject.

It is important to distinguish special category data from personal data, as there are different legal obligations for each of these types of information, particularly in relation to processing. One of the ways in which special category data can be processed is by explicit consent of the data subject.

ADGM Data Protection Regulations 2021

ADGM was established pursuant to Abu Dhabi Law No. 4 of 2013 in the Emirate of Abu Dhabi. ADGM issued new Data Protection Regulations 2021 on February 11, 2021 (**ADGM DPR**). A transition period of 12 months was proposed for current establishments and six months for new establishments, from February 14, 2021.

According to ADGM DPR, personal data is any data relating to an identified natural person or identifiable natural person. It means data related to a living individual who a) can be identified or who is identifiable, directly from the information in question; or b) can be indirectly identified from that information in combination with other information.

The ADGM Data Protection Guideline provides that if personal data can be truly anonymized, then the anonymized data is not subject to the ADGM DPR. Information about a deceased person does not constitute personal data and is not subject to the ADGM DPR. Information about companies or public authorities is not personal data; however, information about individuals acting as sole traders, employees, partners and company directors would be.

An individual is identifiable if they can be distinguished from others. You do not need to know a person's name for that person to be identified/identifiable. Examples of identifiers include names, photographs, ID numbers, location data, a combination of significant criteria (e.g., age, occupation, place of residence) and online identifiers (e.g., IP addresses and cookie identifiers), but there are many others.

Certain types of personal data, known as special categories, receive additional protection because they are more sensitive. For example, the ADGM DPR define the following as special categories of personal data:

- biometric data (where used for identification purposes);
- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- genetic data;
- data concerning health;
- data concerning a person's sex life or sexual orientation; or
- personal data relating to criminal convictions and offenses, or related security measures.

Expected federal data protection law

On September 5, 2021, the UAE announced the introduction of a new federal data protection law. The new law would be the first comprehensive and stand-alone data privacy and protection law in the UAE.

According to H.E. Omar Bin Sultan Al Olama, Minister of State for Artificial Intelligence, the new law forms part of the UAE's Projects of the 50, a set of initiatives designed to mark the country's 50th anniversary. H.E. also stated that "every single data law on the planet" was considered when drafting the law. The new law aims to be a "global law" that provides international companies with a smooth mechanism for cross-border transfers. According to our knowledge, the law is developed in consultation with major tech companies and has been long anticipated.

The new law is expected to bring the UAE closer in spirit to the EU data protection standards under the GDPR. The expected data law will most likely have great impact on the processing and transfer of data in general, including biometric data.

Related Attorneys

Nasser Khasawneh
Partner and Head of TMT
UAE

Christine Khoury
Principal Associate
UAE

Anum Saleem
Principal Associate
Saudi Arabia

Cristina Craciun
Associate
Qatar

Sarah Khatib
Senior Associate
Jordan

eversheds-sutherland.com