Employee Data Gets Promoted:
What are the GDPR’s Impacts on Employee Data, and What Should US Employers Do?

by Michael T. Borgia, David C. Shonka, and Martin T. Tully

I. Introduction

Data privacy has received a lot of attention in recent years. Taking note of the growing public concern about companies’ use (and misuse) of personal data, legislatures around the world have enacted new data privacy laws and have made major changes to existing ones. Probably the best-known recent enactment is the General Data Protection Regulation (GDPR), a broad data protection (and not “just” privacy) law enacted by the 28 countries that comprise the European Union, plus Iceland, Norway, and Lichtenstein. While formally only a European law, the GDPR has garnered significant attention in the United States (and elsewhere around the world). This is due in large part to the GDPR’s sweeping scope, its extraterritorial reach, and the law’s potentially very significant penalties for noncompliance. The GDPR went into effect on May 25, 2018. Many US companies, even those with relatively few activities in the EU, have invested significant amounts of time and money to bring themselves into compliance.

And the GDPR is not alone in fundamentally changing the US privacy landscape. California has enacted the California Consumer Privacy Act (CCPA), which is scheduled to take effect on January 1, 2020. The CCPA borrows a number of provisions from the GDPR and prior EU data privacy laws, and brings those provisions to the US for the first time. Like the GDPR, the CCPA will have significant extraterritorial effects; in the absence of overriding legislation, it will act as the de facto US privacy law. As this is being written, Hawaii, Massachusetts, and Washington State are all considering significant privacy bills. Congress is also studying various legislative proposals, ranging from those offering modest changes to existing laws to those that would overhaul the country’s approach to data privacy.

Public debate about data privacy has focused largely on the business-to-consumer relationship—i.e. on the data collected by companies about the consumers who use their products and services. But data collected through the employer-employee relationship deserves attention too. Employers collect significant amounts of data about their employees, from standard HR and payroll data, to health data, to detailed information about employees’ professional, and inevitably personal,
activities online. It is not surprising then, that the GDPR and other laws (both current and proposed) apply to employee data in many of the same ways that they apply to consumer data.²

Companies working to comply with these expansive data privacy and protection laws must evaluate how they handle employee data alongside how they handle consumer data. In fact, US companies—and particularly those approaching EU data protection law for the first time with the GDPR—may find that bringing their practices in line with new privacy laws is more difficult for employee data than it is for consumer data. Many US companies, whether as a matter of law or policy, have become accustomed to various limitations and obligations regarding their handling of consumer data; in contrast, US companies have considerably less experience, generally speaking, navigating restrictions on how they collect and use data of their employees, particularly when that data is collected at work.

This paper provides a high-level overview of the evolving privacy landscape, highlighting some of the particular challenges that employers face now and may face in the future regarding their collection and use of employee data. Section II describes the basic, traditional tenants of US privacy law in the employer-employee context, and then discusses how the GDPR and new US privacy laws and proposals may drastically alter the legal landscape for US employers.³ Section III analyzes in further detail some common and potentially complex problems that US employers may face when implementing new privacy requirements in the employer-employee context, and offers some specific considerations for solving those problems. Section IV provides a high-level overview of some compliance strategies and tools and analyzes when and how employers might use them to comply with new privacy regimes.

II. Overview of Recent Legal Developments

A. The Traditional US view of Employee Privacy Rights

Traditionally, US law affords employees very little right to keep data private from their employers while they are at work. This is based on two widely accepted legal principles at both the federal and state levels: First, employers own their computer systems and all the data stored on them. Employers therefore have a nearly unfettered right to view and use any of that data whenever and however they see fit. Second, employees are presumed to agree to their employers’ policies as a condition of their continued employment. Employers typically have acceptable use and other internal IT policies stating that employees have no right to privacy when they use corporate systems, and that any data put on those systems is company property. By continuing to work for the employer, employees are generally considered to have consented to those terms, and therefore to have waived any expectation of privacy they have over their data on corporate systems.

² This paper uses the terms “employer” and “employee” in the broad sense, to encompass many types of employment relationships that involve the collection of personal data. Many of the data privacy considerations that apply to legal “employees” also apply to “independent contractors” or other designations. Similarly, many of the considerations here apply equally to job applications and former employees. Analysis of how data privacy concerns may vary depending on the specific nature of the employment relationship is beyond the scope of this paper.

³ It should be noted that this paper’s discussion of GDPR and the other legal regimes is by design broad and simplified. This discussion should not be taken as legal advice and is not suitable for any specific application.
To be sure, US laws place some restrictions on how employers can access and use their employees’ data. Generally applicable data privacy and breach laws govern data collected through the employer-employee relationship; under such laws, employers must disclose their collection and use of data to employees, adopt reasonable security measures to protect employees’ data from unauthorized access, and disclose any data breaches to affected employees. A panoply of federal and state statutes—for example, anti-discrimination and personnel records statutes, and statutes governing biometric data—govern specific types and uses of employee data.

Common law can restrict employers too. For instance, the Pennsylvania Supreme Court recently held that an employer has a common law duty to use reasonable care to safeguard employees’ personal information stored on an Internet-accessible computer. Employers that carelessly disclose sensitive employee data could be subject to invasion of privacy suits. Moreover, as a practical matter, organizations that may not be directly obligated under a privacy law scheme are increasingly finding themselves needing to nevertheless become compliant, due to the expectations of their employees (as well as of their customers and clients).

Ultimately though, these restrictions are the exceptions to the rule, crafted for specific circumstances. Generally speaking, and at least as far as employers handle employee data for arguably work-related purposes, US state and federal laws grant employers broad power to decide when and how employee data is collected; conversely, employees have relatively little say in the matter, especially when they are using corporate systems.

**B. Working with the GDPR**

To understand what the GDPR is about, one has to understand the rationale of many of those who pushed for its enactment. Supporters of the GDPR, and of the EU’s stringent data protection requirements generally, cite Europe’s recent tumultuous history: Decades of totalitarian governments, secret police, non-public (or no) trials, and even summary executions for religious, political, or disfavored speech, associations or activities, arguably have resulted in people in the EU being much more concerned about the misuse of personal information than people tend to be in the US. Today, every government in the EU recognizes that people have a fundamental right to control their personal data and to have an adequate remedy if that right is violated.

This rationale manifests itself in the GDPR in a number of key ways. One such way is in the law’s broad subject matter. The law applies to the “processing” of “personal data.” Personal data is simply “any information relating to an identified or identifiable natural person,” and the concept of processing applies to virtually any kind of handling of personal data, including even holding onto the data for longer than is necessary. The GDPR is designed to give individuals substantial power over data about them—power to decide, often with great specificity, when, how, why and by whom that data is used, and even when it must be corrected or deleted entirely.

---

4 *Dittman v. UPMC*, 2018 Pa. LEXIS 6051 (Pa. Nov. 21, 2018). The Court further held that Pennsylvania’s economic loss doctrine permits recovery for “purely pecuniary damages” on a negligence claim premised on a breach of such a duty.
While the GDPR still is relatively new, it was not cut from whole cloth. From 1995 until 2018, the EU had in place a Data Protection Directive, which contained many of the concepts and requirements now found in the GDPR (meaning that companies that complied with the Directive have a significant head start with the GDPR). The Directive set a floor for the data protection laws of each of the EU member states, leaving member states free to adopt individual, stricter requirements on top of the Directive. This ultimately led to inconsistent applications and inconsistent enforcement. The need, or desire, for a uniform law was one of the main factors in the Directive’s replacement by the GDPR. And while the GDPR did not change many of the fundamental data processing requirements established under the Directive, it did make some significant changes that have caught the attention of US companies and others around the world. The GDPR’s most noteworthy additions include: new and more robust internal processes that companies must follow; documentation requirements concerning the company’s policies, controls, decision-making, and other matters; a more uniform enforcement mechanism; extraterritorial application, including over companies with no physical presence in the EU; and (perhaps most notoriously) the potential for the imposition of very substantial penalties—up to 4 percent of annual word-wide turnover.

From the perspective of a US company approaching EU data protection law for the first time, what is perhaps most astounding and challenging about the GDPR (and of its predecessor Directive) is that the law by default bans all applicable data processing. Companies may only process personal data “if and to the extent” they can show that the processing fits into one of six lawful grounds enumerated in Article 6. In other words, companies can do virtually nothing with personal data unless they can establish that they have a lawful reason for processing the data recognized by the GDPR. Although “consent” is a recognized ground under Article 6, the GDPR’s recitals and formal guidance make clear that the form of consent on which many US companies rely in handling their employees’ data—employees’ presumed consent to company policies by virtue of continued employment—is not sufficient. Under the GDPR’s recitals, consent “should be given by a clear affirmative act” and must be “freely given.” Consent is not considered “freely given” if the data subject is not given the option to agree to some processing but to decline others, or if “the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.” Moreover, consent is not a valid ground for processing where there is a “clear imbalance” between the data subject and the company collecting the data. To the extent the recitals leave any ambiguity, guidance published by the Article 29 Working Party (WP29), an advisory board for data protection issues created by EU law (since replaced by the European Data Protection Board or EDPB), states plainly that “consent is highly unlikely to be a legal basis for data processing at work, unless employees can refuse without adverse consequence.” Although other bases are available to employers, such as the employer’s pursuit of a “legitimate interest,” those alternative bases must generally be balanced against the risks to the employee’s interests in his or her personal information (this legitimate interests balancing test is discussed in more detail in Section III). Moreover, employees (and former employees, as well as every other data subject) have rights to make data subject access requests (often referred to as SARs or DSARs) to access their files, have them corrected, request their deletion, and limit their processing in other ways.
Additionally, the GDPR prohibits companies from transferring data from the EU to the US, except in very particular circumstances and only when the transfer is accompanied with an exacting commitment to protect the data and limit its use in the US. The GDPR also has several provisions specific to employment data. For instance, Article 88 allows member states to enact local legislation that can result in even greater protections for personal data in the employment context than is afforded by the GDPR (meaning that even under the GDPR, companies may continue to have to navigate the conflicting regimes of different member states). Article 9 says that the processing of certain highly sensitive data, such as religious, ethnic, health, and biometric information, is generally prohibited, except where processing is necessary to carry out obligations in the field of employment, insofar as that processing is authorized by the laws of a member state providing “appropriate safeguards.”

To further complicate matters, many US employers—even those with relatively few activities in the EU—may find it enormously challenging to segregate their data processing that is covered by GDPR from their data processing that is not. Most companies have at least some systems, policies and processes that apply to operations and employees around the world—for example, those related to email and other communications platforms, network monitoring tools, or IT and HR helpdesks. Where GDPR-governed data cannot feasibly be segregated from other data, companies may find themselves needing to apply at least some of GDPR’s requirements to all the data involved in that processing. And even where the data can feasibly be segregated, companies may struggle to justify to their workforces why some employees have more rights to control their data than others.

At bottom, operating under the GDPR means that employers do not have broad power to control employee data, as they do under US law. That power must be shared with employees protected by the GDPR—and maybe even those not specifically protected by it—and the employer’s collection and use of employee data under all circumstances must have the employees’ interests in mind. Any claim of assumed employee consent to follow company policies will fall well short. Employers will need to identify and articulate objective justifications for each way they use employee data, and will need to balance their interests as employers in using that data against their employees’ fundamental rights. For US companies just now beginning to grapple with EU data protection law, this may be a strange and arduous exercise. Even for companies well versed in the prior Directive, GDPR’s new requirements, extraterritorial application, and potentially significant penalties may make that exercise a daunting one.

C. The Anticipated Effects of the CCPA

The CCPA will apply to major companies that do business with California residents, even those that do not have physical presences in the state. It will affect how such companies collect, process, handle, and sell or share California residents’ personal data. Upon an individual’s request, companies must give individuals access to their information and must broadly disclose to whom that information is sold, with whom it is shared, and for what purpose. In some circumstances the CCPA will require a company to delete an individual’s information upon request and allow the consumer to opt out (and require children younger than 16 to opt-in) of sales of their data. These types of individual rights are similar to the GDPR’s SAR rights, and are partly why CCPA is
sometimes described as a sort of US variation on the GDPR. The law will forbid companies from
discriminating against consumers who exercise their rights under the CCPA.5

Some have noted that the CCPA’s applicability to employee data is unclear because the law
protects “consumers.” However, the CCPA defines consumers simply as natural persons who are
California residents. Unless a company is prepared to argue that its California-based employees
are not natural persons within the meaning of “natural person,” it should probably regard its
employees as protected by the CCPA.

The CCPA is not as robust as GDPR. In particular, it does not place the onus on employers to
justify each way it collects and uses employee data. Instead, processing personal data is
presumptively allowed except where prohibited by the statute. However, the two laws are similar
in that they provide employees some manner of control—considerably more than is available under
current US law—over how their employers use, share and retain their data.


Given the current public interest in data privacy, it is not surprising that there are a number of
recommendations and proposals for national privacy legislation circulating in Washington, DC,
and there are, and will continue to be, numerous congressional hearings on the subject. But
especially given the current political environment in Washington, it would require a very talented
fortuneteller to accurately predict the outcome.

A few observations, however, can be made. First, many of the core privacy concerns expressed
today are largely related to concerns about technology. Technology makes possible the acquisition
of vast amounts of personal data; and the analysis of that data by that technology makes it possible
for individuals to receive many benefits, large and small, that were largely not even conceivable
only a few years ago. While individuals are often concerned about the privacy implications of
these technologies, they often are equally enthusiastic about the benefits these technologies
provide. Accordingly, even where there appears to be significant momentum to strengthen privacy
laws, it is less clear whether people are willing to accept some of the trade-offs that may come
with those stricter laws. Second, regulating technology is a very difficult endeavor when that
technology is constantly changing. Regulations that sensibly balance privacy interests and the
benefits of technology today might completely miss the mark when technologies change. US
regulators and policymakers have been consistent in expressing concerns about overregulating
technology for fear of suppressing innovation and losing the benefits it provides, along with the
competitive edge technology gives US businesses. Third, the US approach to privacy regulation
largely has focused on transparency and notice, and those concepts remain a core part of many of
the privacy proposals under consideration. The basic rule has been that companies may use

5 In its current form, the CCPA does not allow private rights of action except in data breaches where the breach is due
to a failure to follow reasonable data security practices. There are, however, proposals to broaden that private right,
so it is possible that covered individuals—including employees—may sue for violations of the rights given them by
the CCPA. In its present state, the CCPA will be enforced by the Attorney General, who may seek civil penalties and
injunctive relief in court proceedings. Of course, the ability to seek injunctive relief suggests there is some potential
for the Attorney General to seek equitable monetary relief on behalf of injured consumers, much as the Federal Trade
Commission often has in its consumer protection cases.
consumers’ information when the company has given the consumer notice about how it is using the data, and the consumer consents to that use (or at least does not opt out of it), provided of course, that the company’s disclosures to the consumer are truthful and accurate and relayed in a way that is accessible to the consumer. While the direction of federal privacy law is unclear, this much seems relatively certain: any successful national legislation will need to consider the benefits of innovation, the harms it can inflict on consumers (and the public) by the loss of individual privacy, and the extent to which modern technologies can provide notice that is truthful, accurate and accessible to consumers.

III. Examples of Workplace Challenges Under the Changing Privacy Regime

As noted above, an employee’s consent generally will not be a sufficient basis for processing the employee’s data under the GDPR. For US companies, especially those brand new to EU data protection law, this may create a seismic shift in the way they need to think about their relationship to employee data. Under the GDPR, companies may need to take a much more proactive and detailed approach to analyze, justify and disclose how and why they use employee data than they do under US law.

For the standard processing of HR and finance data—for example, handling the data needed to pay employees, withhold taxes, administer benefits, confirm work eligibility, and the like—these changes ultimately may be much more procedural than substantive. Employers clearly have a lawful basis to process data for such purposes under Article 6’s provisions for processing “necessary for the performance of a contract,” “necessary for compliance with a legal obligation,” or for processing “necessary for the purposes of the legitimate interests pursued by the controller.” Employers will need to document and disclose such processing activities to employees, and will need to be prepared to respond to employee’s data subject access requests concerning that data; however the actual processing activities should remain largely unchanged.

Things may get more complicated from there, particularly when the employer’s and employee’s interests diverge. Take for example, data processing to track employees’ job performance, monitor employees’ behavior for bad conduct or data loss, or to make decisions about hiring, firing, promotions, etc. Undoubtedly, an employer has some “legitimate interests” under the GDPR in processing data for each of these purposes. Employers need to understand how their employees are performing, to ensure that malicious activities are not being conducted on their network, and ultimately to decide whom to hire, whom to fire, and whom to promote. But “legitimate interests” are defined objectively under the GDPR—employers are not free to define their interests as they please and process data accordingly, but rather need to identify interests that are considered legitimate under the regulation, and then tailor their processing to those recognized interests. As noted above, the burden rests with employers to demonstrate that their processing of employee data is lawful.

Official guidance describes Article 6’s “legitimate interests” provision as imposing a three-part balancing test on employers (or other data controllers). That provision states that processing is lawful to the extent it is:
Thus, for each type of processing of employee data, the employer must: (i) identify its own legitimate interests for which the processing is necessary; (ii) identify the interests or fundamental rights and freedoms of employees implicated by that processing; and (iii) balance the employer’s and employees’ interests to determine whether the processing is justifiable under the regulation. The stronger and clearer the employer’s interests (e.g. paying employees or delivering services to customers), the more likely the processing is to be lawful. Conversely, where processing creates a risk of harming employee interests (e.g. maintaining privacy over personal affairs, maintaining control over their data, etc.), employers will need to make especially strong showings that the processing is necessary and tailored to legitimate business needs.

A. Compliance Monitoring and Investigations

The WP29 provided guidance on the processing of employee data ahead of the GDPR coming into effect. That guidance discusses the legal issues and considerations around the deployment of monitoring tools for corporate IT systems, such as data loss prevention (DLP), firewalls, application logs, and mobile device management (MDM) software.

One point that emerges from the WP29 guidance is that while employers undoubtedly have legitimate interests in monitoring incoming and outgoing traffic for security threats, data loss, etc., any type of monitoring system that processes employee data must undergo GDPR analysis to determine whether such processing is lawful. Where the employer is citing Article 6’s “legitimate interests” provision to justify the processing, it must employ the aforementioned balancing test to answer several questions:

- Are the monitoring tools under consideration necessary to protect against security threats, data loss, or other legitimate risks?
- Is the data processed by those monitoring tools appropriately limited to data that needs to be processed to protect against those risks?
- Are there other, more limited tools or mechanisms that could be used to protect against those risks?
- Is there a way to avoid storing employee personal data, or at least avoid storing employee personal data that is not connected to any threat indicators?
- Is there a way to configure the monitoring tools to reduce the number of false positives? This is particularly relevant for DLP software, which potentially can flag or block significant amounts of legitimate traffic if configured too broadly.
- Can certain types of potentially sensitive traffic, such as to webmail or online banking portals, be excepted from monitoring? One possible solution raised by the guidance is providing a dedicated personal/guest network for employees to use for personal web traffic.

The WP29 guidance further states that, regardless of the tools implemented, employers must be transparent with employees: about how employees may and may not use corporate IT systems (but
note that a blanket ban on use of corporate IT systems for any personal reasons would rarely if ever been seen as permissible under the GDPR); how and when employee activities will be monitored; and the nature of the data processing that will take place. Employers will need to balance the employees’ interest in transparency against the employer’s need to keep some of its detection and defensive measures secret from would-be threat actors. For example, employers will need to be transparent about the use of DLP, the types of data it detects, and the types of endpoints on which it is used, but will want to avoid providing so much detail that the employer effectively gives threat actors a roadmap for exfiltrating data without triggering a DLP alert.

Security investigations and other investigations of potential malfeasance present especially thorny challenges, particularly where an employee is the subject of the investigation. These investigations are dynamic in nature, and so the actions that need to be taken and the evidence that needs to be reviewed can change by the minute. Accordingly, when investigative activities involve the processing of employee personal data, employers may constantly need to apply the “legitimate interests” balancing test at each step of the investigation, based on the evidence available at each point in time.

Consider, for example, an investigation of an employee suspected of removing intellectual property from the corporate environment and misappropriating it by starting a rival company. Under US laws, the employer has nearly free range to investigate any corporate systems, including the employee’s work-issued laptop. Little to no consideration of the employee’s privacy interests is necessary, as the systems and all data contained therein are considered to be property of the employer. The investigation team generally is free to examine whatever it wants, and may even conduct generalized searches to see if the employee has committed other, entirely unrelated, malfeasance.

Under the GDPR, the legal analysis is considerably more complex. If the investigation team decides that a review of the employee’s laptop is needed, the company will need to analyze—and should document—the company’s legitimate interests in searching the laptop, whether the search of the laptop is necessary to those interests, and whether there are less intrusive ways the company could achieve those interests. The outcome of this analysis will depend in part on the nature of the evidence to date and the inferences from that evidence. For instance, if the employer has received DLP flags suggesting that PowerPoint files marked “highly confidential” have been uploaded to a USB device, the employer may justifiably be able to search the laptop for evidence of PowerPoint files leaving the computer. But the employer would not necessarily be able to generally investigate endpoint activity to determine if other types of sensitive data stored in other types of files had left the computer. Based on the initial DLP flags, the employer may not be able to establish that its interests in the investigation are sufficient to overcome the employee’s privacy interests in the other data and activity on the device. However, if in the course of looking for evidence related to the PowerPoint files, the company discovered that the employee appeared to be uploading customer data in Excel files to a USB device in violation of corporate policy, the company could reapply the legitimate interests balancing test and may be able to justify expending the investigation to search for evidence around misuse of those types of files.
To save time during investigations and to make sure the company is applying the balancing test in similar ways under similar circumstances, employers should take stock of the common types of security incidents they face and the evidence they may need to review for each type. For example, with respect to employees’ corporate laptops, an employer could document when and why the employer might need to access those devices, the employees’ interests with respect to the data on those devices in light of corporate policies, legal rights, and other factors, and how the processing of data on those devices can be minimized to properly balance the employer and employee’s interests. That general analysis could then serve as a sort of template for the analysis in specific investigations involving review of corporate devices. Similar general analyses could be conducted for firewall logs, DLP flags, database trace logs, web browsing history, and other common technical artifacts.

B. Tracking Employee Job Performance

Tracking employee job performance is as essential for employers as it is risky under the GDPR. On the one hand, no one doubts that employers need to assess their employees’ performances. On the other hand, tracking performance can sometimes intrude on employee privacy, and other times employee job performance information can get captured in surprising ways. Several examples may illustrate the problem:

- A taxi service decides to track its cars in order to be efficient in answering customer calls and to minimize fuel consumption (and resulting pollution); but the data used to track cars might also be used to show that a particular driver is unconcerned about either efficiency or pollution and is sometimes making unscheduled stops for inappropriate, wholly personal, reasons.
- A firm might use surveillance cameras to secure its parking lots and entrances; but the resulting images may also show that a particular employee is consistently tardy or is taking unscheduled breaks from work.
- A manufacturer may wish to monitor its machines or production lines to ensure they are functioning properly; but the data that shows a particular machine or production line is less efficient than others might instead show that the operator is being distracted by a co-worker.
- The same manufacturer decides to install facial recognition devices or fingerprint scanners for timekeeping purposes; but such a system entails the collection and use of sensitive information that is likely covered by Article 9 of the GDPR.
- A multinational company may wish to consolidate all its employee data into a single US database for processing and record-keeping purposes and to gauge the output of its various facilities; but that very process will identify individual productivity and entail both the processing of personal data in ways that may be prohibited by Articles 6 and 9 and the transfer of personal information outside the EU on its face triggers major concerns with the transfer mechanisms established by Articles 44-49.

These are only a few of the possible scenarios; the possibilities are infinite. And although the EU has not yet published guidance that provides a definitive solution to these issues, it is likely possible to tease out answers, or at least workable solutions, to many of them with a careful
analysis of the exact purposes and circumstances involved. There are a few points that employers always should keep in mind: First, whenever a company employs new processes (or extends existing ones) that may present a substantial risk to the privacy rights of data subjects, the company must first conduct a detailed Data Protection Impact Assessment (DPIA), which is a detailed critical analysis of its reasons for processing the data and its systems to protect the data. Second, whenever a company collects personal data, it must deploy “data protection by design and default,” as described in Article 25 of the GDPR. This essentially means that the employer must design its processes to collect and process the minimum amount of data necessary for the intended purpose. Third, the GDPR requires all major decisions with respect to processing be documented in writing. Fourth, as noted above, the GDPR expressly allows individual member states to develop additional regulations to protect employee rights, and all such regulations must be consulted and obeyed (following the GDPR alone is not sufficient). Fifth, in some EU countries, companies may be expected to engage in discussions with works council(s) and obtain their agreement.

With a few exceptions, such as those involving criminal misconduct, a best practice under the GDPR is for employers to be as transparent as possible with employees and ensure that their GDPR rights are fully protected. In the context of tracking job performance, employees should know what information the employer is collecting, the reasons for the collection, the precise way in which the information will be used, and how long it will be kept. Employees should also be assured that they can assert all their rights under the GDPR with respect to the data. As already noted, employee consent is rarely if ever a sufficient basis for processing employee data under the GDPR, but employees must be informed of what the employer is doing and be allowed to assert all their rights, including the right to object and the right to correct their data.

C. Automated Decision-making

Article 22 of the GDPR states that “[t]he data subject [i.e. the employee] shall have a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her,” except under limited circumstances. This general prohibition on solely automated decision-making could affect various types of data processing activities across the organization.

Guidance from the UK Information Commissioner’s Office (ICO) explains that solely automated decision-making is decision-making that “excludes any human influence on the outcome.” While the term “solely automated decision-making” may invoke images of advanced artificial intelligence, common examples are much simpler. For instance, basing an employee’s compensation entirely on an automated report of how many customer orders that employee processed in a given time is considered solely automated decision-making under the ICO guidance. So too is an employer’s decision to interview certain job candidates over others based entirely on an online aptitude test, or an employer’s decision to terminate an employee based solely on the records of an automated attendance system.

The general prohibition on solely automated decision-making also implicates the security organization. For example, using DLP to automatically block employees from removing certain files from their corporate laptops could be considered a violation of Article 22. Consider, for
example, a situation in which an employee is not able to remove important personal financial documents from his or her work computer because of DLP blocking.

Fortunately for employers, the ICO guidance indicates that this prohibition can be addressed by adding even a relatively modest amount of human decision-making. Take for example the situation where an employee’s compensation is based on an automated report on orders processed. The ICO guidance indicates that this decision-making would be permissible as long as a supervisor meaningfully reviews the data generated by the report and then decides on the employee’s compensation. The supervisor does not need to base his or her decision on other factors beyond what is in the report. However, the human decision-making cannot simply be a rubber stamp of the automated report; the ICO indicates that a key consideration is whether the supervisor has discretion to alter the decision taken by the automated system before it is applied. For DLP or other information security measures, employers might consider implementing a process whereby an employee can request manual review of endpoint blocking or other automated decisions.

D. Employee Data Subject Access Requests

As noted above, the GDPR and the CCPA provide data subjects several enumerated access request rights to understand and control how their personal data is processed. Such requests may present significant challenges for employers with respect to data that they typically do not share with their employees.

Consider for example the following scenario: an employer processes employee performance data in order to conduct a year-end review and to determine promotions and compensation. This performance data includes reviews by employees’ peers and supervisors. Those reviews and other performance data generally are not shared with employees; rather, employees generally only receive performance ratings on various metrics and annual compensation figures.

An employee whose personal data is governed by the GDPR or the CCPA is entitled to make a data subject access request to obtain copies of the data underlying the performance review and decisions, including the other’s employees’ statements. Particularly under the GDPR, the employer’s ability to decline to provide copies of that data is extremely limited, such as to where the request is “manifestly unfounded or excessive” or where disclosing the data would “adversely affect the rights and freedoms of others.” Generally speaking, employers will need to be prepared to share such data with employees who have rights under the GDPR, and potentially under the CCPA too. Employees have the rights under the GDPR to request that such data be rectified or deleted where the data is “no longer necessary in relation to the purposes” for which it was collected, and similar rights to rectification and deletion exist under the CCPA. For example, an employee could request that the employer delete a negative performance review from several years ago on the grounds that it is no longer necessary to evaluate the employee’s performance. Responding to data subject access requests can be even more complicated when the employee requests data collected as part of a disciplinary investigation against that employee.

If only part of an employer’s workforce has these kinds of legal rights, the employer will have to navigate the fact that some employees will have greater legal rights to access and control their data than others. These differences are not theoretical—they can mean, for example, that some
employees will have greater ability to access and scrutinize the data underlying their performance reviews and compensation than other employees. As a matter of policy, companies will need to decide whether to extend such rights to all employees (for example, by increasing transparency into the review process for all employees), or simply to deal with any fallout from employees who may find themselves at a disadvantage vis-à-vis their colleagues with GDPR or CCPA rights.

IV. Strategies for Compliance

It may seem as though each year another new privacy law framework comes into play, and that companies always are playing catch-up. And, as discussed throughout this paper, significant differences exist in EU and US laws governing how employers can collect and use employee data. The easiest way to navigate this seemingly dizzying array of privacy laws is to focus on what those laws have in common and build from there. For example, the GDPR, the CCPA and other privacy requirements compel companies to know what types of personal information they possess and where. In addition, laws focusing on data security and privacy all have at their core the necessary acknowledgment that a sufficient level of data security maturity is required to achieve baseline compliance. Indeed, maintaining a reasonable data security program is a best practice regardless of which privacy laws may be applicable, and even if none are

Other requirements found in various privacy and security statutory frameworks include:

- Providing for a consent mechanism for data subject opt-in or opt-out of processing or sale of personal information
- Providing specific information to data subjects such as purposes of processing data, contact information, existence of certain consumer rights, and providing a link for opt-out requests or opt-in consents
- Providing data subjects with access to their personal data
- Accommodating a data subject’s right to request that information about the data subject be deleted
- Providing for data portability
- Notifying data subjects of any sharing of their personal data with third parties

The common threads in various data security and privacy statutory frameworks, like the GDPR, the CCPA, the New York Department of Financial Services’s (NYDFS) Cybersecurity Regulations, and others offer some practical take-aways regarding how to better prepare your organization for compliance.

Data Inventory & Mapping. At the outset, it is critical to understand what information your organization is collecting, for what purposes, how is it kept, how is it used, and who it may be shared with. An important first step is to conduct a data mapping/data flow analysis to inventory your data and understand what types of regulated personal data your organization collects and maintains, and the other key things you need to know to comply. What is the personal data, and where is it? How is it being used and why? Organizations need to understand the obligations and circumstances of data collection, and cascade those throughout the entire company. Mapping
sensitive data elements across key applications can improve company operations and accelerate its path to becoming compliant with any privacy law.

**Risk Assessment.** Conduct risk and privacy assessments across all governance programs, people, processes, data, and security environments. Document these assessments as new processes are developed and implemented—for example, conduct a DPIA under the GDPR, which can be leveraged elsewhere. Bake in privacy from the start, and do not simply add it on later. This can mean revisiting and redesigning old business models and customer interactions.

**Documented risk-based controls.** Design and implement privacy, data management, and security management controls tied to your risk assessment. Think in terms of data protection by design and by default. It is vital to “tell a good story” about why you have in place the controls that you do, and why you don’t have others in place.

**Access and transparency.** Data privacy concerns arise wherever personal data is collected, stored and used. Requirements here are more legal than technical. Specific processes will be needed for responding to data subject requests, including for legal analysis regarding which data must and need not to be disclosed or shared. Ensure that policies, terms and conditions, access and use, are clear and transparent around-the-clock to clients and customers, who can then revoke or change consents at any time.

**Anonymization, pseudonymization, and aggregation.** The GDPR recognizes the privacy-enhancing effect of these techniques by providing exceptions to many of the most burdensome provisions of the regulation when steps are taken to de-identify personal data. By making it impossible or impractical to connect personal data to an identifiable person, data controllers and processors are permitted to use, process and publish personal information in just about any way that they choose. These same techniques can be leveraged to comply with other regulations, such as the CCPA. Anonymized data must be stripped of any identifiable information, making it impossible to derive insights on a discreet individual, even by the party that is responsible for the anonymization. When done properly, anonymization places the processing and storage of personal data outside the scope of the GDPR. Pseudonymization is defined by the GDPR as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.” By holding the de-identified data separately from the “additional information,” the GDPR permits data handlers to use personal data with less fear of infringing the rights of data subjects. This is because the data only becomes identifiable when both elements are held together. Aggregated data is information gathered and expressed in a summary form for purposes such as statistical analysis, and so is not personal data for the purposes of data protection laws, such as the GDPR.

**Data minimization.** Another important principle in the GDPR is data minimization. Data processing should only use as much data as is required to successfully accomplish a given task, and for only as long as it is needed to do so. Organizations must limit personal data collection,
storage, and usage to data that is relevant, adequate, and absolutely necessary for carrying out the purpose for which the data is processed. Additionally, data collected for one purpose cannot be repurposed without further consent. Data minimization also has the advantage of reducing the risk that protected information will be subject to a data security incident by keeping less of it for a shorter period of time. If the organization conducts a good faith, reasonable investigation and does not find that it has a legal requirement (based on statutory or regulatory obligations) or a business need to retain the information, and is not subject to preservation obligations arising out of litigation or government investigation, the organization is under no duty to continue to retain the information and may securely destroy it.7

**GDPR gap analysis.** If your organization is already GDPR compliant, you are not off the hook. You should conduct a gap analysis against new laws like the CCPA to determine if there are additional requirements unique to that statute, such as the mandatory “do not sell my personal information” link on the businesses website homepage and the CCPA’s anti-discrimination provision, that need particular attention.

**Third-party vendor management.** Review and revise as needed relevant third-party contracts to insure that third-party vendors and others in your organization’s “supply chain” are also compliant, especially where they process personal information for which your organization is responsible.

**Security of personal data.** Securing data against unauthorized access is a cornerstone of any privacy framework and compliance program. These involve adopting mostly technical measures for providing and securing of personal data while it is in your organization’s possession, custody or control. Ensure appropriate encryption, access controls, monitoring and masking are in place end-to-end. Another important practice is to develop and periodically test a proportional and effective data security incident response plan.

**Audit and Adjust.** Monitor, assess, audit, report and evaluate adherence to privacy standards. Monitor technical and organizational measures and deliver compliance evidence to internal and external stakeholders.

**Compliance timeframe.** The laws will keep changing, so you need a program that can monitor legal and technical development and makes necessary changes as appropriate.

**V. Conclusion**

The GDPR and other new privacy laws fundamentally change how many US employers will need to handle their employees’ data. While compliance with these laws is a daunting task, employers would do well to focus—at least as an initial matter—less on the specific requirements of each law and more on implementing the foundational requirements that many of these laws share. Any organization that provides its employees with meaningful notice and choice about how it uses

---

7 *See Arthur Andersen, LLP v. United States*, 544 U.S. 696, 125 S. Ct. 2129, 2135 (2005) (“‘Document retention policies’… are common in business” and those policies “are created in part to keep certain information from getting into the hands of others, including the Government”).
employee data, and that incorporates employees’ privacy interests into its decisions as a matter of course, will be far down the road to compliance.