Bloomberg Law®

The New Normal for Employee Privacy Expectations After GDPR

International HR Decision Support Network™

Bloomberg Law's resources will change the way you do business.

The “New Normal” for Employee Privacy Expectations After GDPR

By Robert Lewis, Partner, and Yana Komsitsky, Associate, Baker McKenzie LLP

Mr. Lewis is a Partner at Baker McKenzie’s New York Office, where he focuses his practice on international and domestic employment counseling and dispute resolution.

Yana Komsitsky is an associate in Baker McKenzie’s Palo Alto office, where she focuses her practice on domestic and international employment and data privacy law.

Many viewed the highly anticipated coming into force of the European Union's General Data Protection Regulation (“GDPR”) on May 25, 2018 as the "finish line" for the marathon efforts towards privacy compliance that took place in the months running up to this date. In reality, however, this date should be treated instead as a "starting line" from which to launch mandatory organizational protections for the personal data of individuals in the EU and elsewhere going forward.

Most companies with European operations have spent at least two years preparing for the GPDR. These often extensive - and expensive - efforts were typically led by companies' legal, compliance, IT and security departments, and/or privacy offices, if any, and were supported by outside counsel and privacy consultants. The efforts often prioritized commercial or business data processed by the companies (through the websites, products, business contracts, etc.) instead of the data of employment candidates, employees, and other workers, such as temporary agency workers and independent contractors (collectively, "HR data"). This article will briefly discuss the basic steps organizations were required to implement for the GDPR, but primarily focus on the work that should continue for HR data compliance from this point on.

This ongoing work will typically fall within the ambit of HR professionals and others who are responsible for management of global HR data (or privacy compliance generally). A common frustration with prior GDPR "readiness" efforts is that those charged with leading them often

did not have enough insight into the nuances of HR practices and common employee privacy issues, including some of the carve-outs and exceptions to the general rules that must be applied in the employment context (e.g., the inability to rely on employee consent for most purposes). At the same time, HR managers often suffer from a lack of visibility into the details of broader organizational compliance efforts (e.g., they have been told data transfer agreements are in place but not told which exact purposes such agreements cover). The end result can be gaps in compliance in respect of HR data and HR processes and the lack of a comprehensive plan for ongoing compliance, which in turn can carry the risks of fines, claims, and employee as well as public relations issues.

HR Professionals Are the Primary Advocates for HR Data Protection

Commercial data-related violations may get more attention, but HR data-related violations can be just as damaging to a company's image and brand, employee relations, or bottom line. Employees are often the source of both breaches and complaints and are now, more than ever, sensitized to their privacy rights and expectations. As the primary custodians of HR data within any multinational organization, HR professionals must be cognizant of their ongoing responsibilities for HR data and take an active role in advocating its protection as HR data privacy advocates. This often requires active engagement with marketing, IT, and procurement teams, who may overlook certain HR data and may not be aware of the interplay with local employment law requirements.

The role of HR data custodian should not be overwhelming. Many GDPR principles are not entirely new. They have long been European law under legislation that existed prior to the GPDR– the Data Protection Directive and corresponding local privacy and employment laws. In practical terms, this means that in the HR arena, most pre-existing processes and privacy documentation can be leveraged and updated for GDPR compliance. There is no question, however, that under the GDPR, the requirements are often more onerous, enforcement is expected to be stricter, and fines heavier. Accordingly, merely relying on pre-existing processes and privacy documentation is not a viable option. Further, the GDPR is intended to “harmonize” privacy laws but it also allows for country specific distinctions in the employment context. As a result, companies utilizing "one-size- fits-all" global or regional approaches and documentation when addressing candidate, employee, and other worker privacy issues should reconsider and monitor changes in local (not just pan-European) law on an ongoing basis. The GDPR specifically allows for supplementing local laws by each EU member state and these continue to come online.

Does the Organization Have the Basic Steps Covered?

Step 1: Understand how HR data is collected and where it flows.

There is often a tendency, especially within U.S. multinational companies, to overgeneralize in privacy documentation and to try to solve noncompliance issues by giving notice or seeking consent to otherwise noncompliant practices from employees and other workers. Copious guidance has been published by the European data protection authorities condemning overgeneralized statements because they are not sufficiently transparent. Consent is only appropriate to seek from an employee in very limited circumstances where the employee has a true choice. The GDPR's increased emphasis on transparency requires a very thorough understanding of the HR data collected, processed, and stored by an organization. Generalized statements are not enough to be compliant.

Those with oversight of global HR functions must fully understand what HR data is collected and where such data goes once collected. Comprehensive understanding of data collection points and flows is not only required to produce the mandatory "records of processing" in respect of HR processes, but is also the best method to avoid an overgeneralization problem in privacy documentation and to determine when the so-called "Data Protection Impact Assessments" ("DPIAs") are required. Because the GDPR (and many other laws) defines personal data broadly (generally speaking covering "any information relating to an identified or identifiable" individual), HR data includes a host of information that is commonly collected and maintained by employers, including, work and home contact information, salary and benefits, badge data, IT and phone use data, photos, video and surveillance footage, among other things.

For a U.S.-based multinational company, it is necessary to understand not only how and where each data category is collected and stored in the country of origin, but also how each category is "transferred" elsewhere and for what purposes. Data is considered "transferred" if it is accessible outside of the home country. U.S. multinationals often send most data to the U.S. for processing, decision making and record keeping. Accordingly, the U.S. parent company must be identified as a recipient (and sometimes it collects HR data directly into the U.S.). Other affiliates and third parties who handle data should also be identified, but the purposes for transfer to affiliates are likely more limited. These can be fairly obvious (such as regional European headquarters, HR hubs, or business support centers processing data for HR and compliance purposes) or not so obvious (an affiliate or vendor located in a third country such as India processing data for data storage or back up). To meet the GDPR's high transparency expectations, the data flows must be described in sufficient detail in privacy notices to candidates, employees, and other workers.

Transparency also requires the mechanisms for safeguarding any transfers are explained to employees (which means such safeguards must first be put in place to avoid misrepresentations).

Step 2: Data processing and transfer agreements should cover all HR data.

Overgeneralization is also commonplace in data processing and transfer agreements. There is often stronger justification to share commercial/business data more widely within the group of companies and much less justification to share HR data that broadly. Accordingly, group data transfer or processing agreements (as well as practices) tend to overgeneralize with respect to HR data because they were often prepared with commercial data rather than HR data in mind.

A typical problematic area arises with respect to global unfettered HR Information System access. Whereas it may be possible to justify some access for a U.S.-based HR lead, an APAC HR manager with no oversight over European employees should not have access to European HR data. Ideally, only HR and other managers with direct oversight over the relevant European data subjects should be able to access the HR data of those individuals. Other access usually cannot be justified and should not, therefore, be expressly documented or implied in a group data transfer agreement (i.e., the agreement should not state that all affiliates receive all HR data, without further detail or breakdown). Companies should strive to minimize unnecessary or unfettered access and ensure that actual practices are documented in group data transfer agreements instead of being overly inclusive.

For example, *employee directory data* may legitimately be transferred to all group entities for communication and collaboration purposes, but *salary information* for European employees typically may only legitimately be transferred for operational purposes to the U.S. headquarters but not to other affiliates. Each type of data transferred should be assigned a purpose in the data transfer agreement and not transferred if there is no legitimate purpose for such transfer or access. Very general purposes such as “organizational or business needs” are frowned upon by the data protection authorities as such needs are often deemed capable of being met in the home country.

Many group data transfer agreements provide for a modification mechanism so that minor changes/additional data categories or transfer purposes will not require entirely new agreements or multiple re-executions. Accordingly, this should not be a reason to avoid making improvements, given that data protection authorities, employees, and others have a right to request and review these agreements.

It is also important to remember that every vendor with access to HR data should have signed a data processing agreement, including those that are currently located in Europe or are "Privacy Shield certified" (the terms of such agreement might change depending on the precise circumstances). There is no excuse or exemption for failure to put written terms in place with any data processing vendor, regardless of how long the vendor has had access to the organization's HR data. Equally, vendors should not be permitted to hold onto HR data if they no longer provide the services which required the data shared. Further, not all vendors are "processors," and the "controller" versus "processor" status of any given vendor may be the subject of some debate with that vendor. The analysis and appropriate terms should be built into the vendor procurement process for new vendors. The legal department may need to be involved.

Step 3: Appropriate privacy notices for all processing activities involving HR data should be issued - one all encompassing notice is not enough.

Candidates, employees, contractors, and other workers must be notified of the company's data practices. For most workers, such notice should come from the local employer and should explain in detail what data is collected, the purposes for collecting it, where it is transferred, the rights individuals have with regard to their data, among other items. The GDPR sets out a number of information requirements that were not required in existing pre-GDPR notices. As a result, historic pre-GDPR notices would obviously be deemed insufficient in case of a GDPR compliance audit or complaint. In the run up to the GDPR (and sometimes shortly thereafter), European employees received countless such notices from other organizations with whom they have interacted (from their dentist to the local supermarket loyalty scheme), so they now expect a certain level of detail from their employers.

Not all data handling may be covered in a single privacy notice. For example, CCTV, IT monitoring activities, and the compliance hotline typically require separate notices with country-specific nuances. If the U.S. parent company separately collects and processes HR data (for example, in the context of granting equity and running equity schemes), it may need to issue a separate notice but must be careful to avoid taking on an employer role by virtue of that notice to protect itself from unnecessary (joint or otherwise) employer liability. If the U.S. parent company certifies under Privacy Shield with respect to HR data, it should issue a separate notice addressing the Privacy Shield requirements.

Step 4: Procedures for "Data Subject Access Requests" from candidates, current, and former workers should be implemented

Any candidate or any current or former worker may request certain information concerning the data that the company holds concerning any of them, triggering a time limit within which the company must respond. Privacy notices should clearly direct such requests to a central contact. Such requests, however, can typically end up with HR and other managers and may not clearly reference the GDPR or privacy rights. This does not necessarily invalidate the request although it may be necessary to seek further clarification or narrowing of the scope of the request. Employees who are likely to receive such requests (which, depending on organizational structure, could include managers, office managers, and others) must understand that these requests cannot be ignored, are subject to a time limit for response, and must, therefore, be escalated accordingly.

Step 5: An easily accessible incident response plan to be used in case of security breach or data loss should be in place.

Many companies have implemented elaborate incident response plans which often are comprised of documentation and procedures housed within the IT or cybersecurity departments. These have a place and purpose but are of little use to the average employee who may suddenly realize that he/she has left his/her laptop or documents on a train, experienced a break in at home or in the car, or accidentally forwarded an email to an unintended recipient. To facilitate the company response within the required 72 hours, all employees should know what is required of them when something like this happens. The instructions should be brief (e.g., a contact email and phone should be prominent, well socialized and easily found on company resources such as in handbooks, on the intranet, etc.). No employee should be able to credibly say, "I didn't know how to report the incident."

Step 6: Make sure the training program for HR data handlers does not go stale.

Others within an organization may have access to HR data and also have ideas on what to do with it. This could be a marketing person who decides to "dry run" a marketing initiative on employees, an IT team that wants to roll out new monitoring measures for security purposes, or a recruiter who decides to pool from candidates from years past. All of these initiatives should raise privacy red flags. A training program addressing some of the more common uses (with examples relevant to the target audience) can help ensure that privacy rights are taken into consideration and addressed before such initiatives go live and cause irreparable damage.

Trainings and refreshers should be repeated at appropriate intervals and made available to new joiners, those returning from leave, etc.

How to Ensure Compliance Going Forward

GDPR compliance requires making privacy integral to every process. The GDPR and its corollary rules are the new normal, encompassing ongoing compliance obligations. Even if an organization has completed the basic steps outlined above, there is always more to do. As custodians of HR data, HR professionals must ensure that worker privacy is considered and safeguarded in all data handling and worker monitoring activities.

To maintain compliance, HR managers and others with responsibility for HR data must continuously look out for "gaps" in existing processes and design privacy considerations into any new processes to be implemented. If there are works councils or other employee representative bodies within the organization, they will often need to be informed and consulted (in some cases an agreement will be required) before new processes or new data sharing may commence. "Data Protection Impact Assessments" may be required before certain types of "high risk" processing may begin. Some processing activities may still require DPA approvals. Often, the precise rules can vary by country.

Some of the most common scenarios where privacy rules are implicated but easily overlooked are:

- **During the hiring process with applicant / candidate tracking systems**
  Applicants should receive their own comprehensive candidate notices from an employer on its job portal or wherever candidates submit their data for the first time because that is when their data is first collected --before they become employees and receive employee privacy notices. It is not recommended to assume that the ATS vendor has taken care of this on the employer's behalf.

- **Background checks**
  Background checks are usually conducted before the individual receives an employee privacy notice and the specific rules vary greatly by country. Again, it is not recommended to assume the vendor has taken care of this on the employer's behalf, especially if contracting with a global vendor. Merely providing the individual's contact details to the vendor can be problematic from a privacy perspective and consent from the individual does not necessarily mean the check will be lawful or adequate.

- **Contractors/contingent workers**
  Nonemployee workers are entitled to the same level of transparency but should not receive employee-style privacy notices (and there should be no mention of payroll, benefits, etc. in the notices they receive). With these groups, it is important to consider which entity is the engaging entity and the data controller on a case-by-case basis, in order to provide the correct notice.

- **CCTV/video surveillance use**
  European and other courts have recently been very critical of employer use of video surveillance. Whether an employer can legitimately utilize covert or overt video surveillance depends on the specific purpose and location of the cameras on the employer's premises, and certain approvals may still be required prior to implementation. In any case, notices should be displayed on location so that the individuals being recorded can see such notices before stepping into the area where recording is taking place.

- **Compliance or ethics hotlines**
  Even if the organization has rolled out a global compliance hotline in the past, it should update the hotline for compliance with the new privacy rules and changes in local anti-corruption law. France and Germany are two countries that have recently implemented significant changes to expectations for U.S. compliance hotlines, with German rules changing drastically following the GDPR. It is not recommended to assume the hotline vendor will keep the organization in compliance and companies should expect the vendor to take some time to implement the requested modifications to the hotline facility.

- **Acceptable Use Policies, IT Security Policies, and BYOD or mobile devices policies**
  European employees (and those in many other locations) have an expectation of privacy in their use of their employers' systems that cannot simply be waived or negated with a general statement on a splash screen or in the employee handbook. Global or U.S.-style policies on these topics are very likely to breach some local laws on their face (undermining any value in having such a policy) and should be localized or at least regionalized accordingly.

- **Marketing initiatives, voluntary activities (e.g. product testing), or employee surveys**
  Particular attention should be paid to initiatives and surveys concerning sensitive topics like diversity and inclusion or those that use employee photo images. These require comprehensive advance disclosures about the intended uses of the information

collected, among other things, which usually cannot be adequately addressed in a general employee privacy notice.

- **Any M&A related data sharing or transfer**
  Those in an organization in charge of M&A and their advisors may not have HR data at the top of their list of concerns, even though HR data is typically some of the first data shared in a typical M&A transaction lifecycle. Data transfer agreements may be necessary. Data minimization and delay of transfer to the later stages of the transaction are key risk mitigation strategies.

- **Record retention policies and schedules for employee records**
  An organization may have a global record retention schedule or it may not (effectively retaining information indefinitely). Both approaches can fall short of compliance as the GDPR requires that HR data is only retained as long as necessary for the purpose it is collected. This means that a candidate interview file will generally be required to be deleted much sooner than a health and safety record that is required to be retained for a statutory period in a given country. If the two records are comingled in company systems, it may be necessary to separate the records. Several options exist for balancing global operational needs with GDPR and local record retention requirements, but the ultimate solution depends on technical capabilities of company systems, company preferences and risk tolerances.

What About Non-European Employees?

Given the extensive resources and process changes required for GDPR compliance, organizations should consider whether to combine these efforts or expand them to cover HR data for the rest of the world. Privacy laws (often modelled after the European framework but implemented with important differences) now exist in nearly all commercially-significant countries and continue to come online in some unexpected places. The thought processes are largely the same, even if the procedures and policies ultimately implemented may require some modification (for example, in countries that do not reject the use of consent with employees).

Some jurisdictions (for example, Russia, and soon, India) have additional “data localization” requirements that serve a somewhat different purpose but can be efficiently addressed at the same time as privacy compliance.

Conclusion

It is important for HR professionals to remember that even though GDPR readiness exercises may have been completed in May 2018, GDPR compliance obligations are ongoing. Global HR professionals must maintain vigilance and always ask:

- Is HR data implicated in the existing, new or changing initiative or process at hand?
- What steps are required to ensure that the initiative or process does not breach GDPR or other privacy laws, depending on where the impacted individuals are located?

Most initiatives are still possible within the confines of the new rules. It is a matter of building into them the required protections and possibly making some modifications globally, or on a country specific basis. Most multinational companies handle HR data in very similar ways and share the same concerns and frustrations when developing programs to comply with multiple privacy laws, including the GDPR. Working with experienced employee privacy counsel can help an organization find practical solutions to compliance by leveraging the tried and tested approaches taken by other companies facing the same compliance predicaments.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of Baker McKenzie, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

About Baker McKenzie

Baker McKenzie helps clients overcome the challenges of competing in the global economy. We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients. (www.bakermckenzie.com)

Baker McKenzie's Global Employment & Compensation group is one of the world's largest and most recognized employment practices, with more than 700 lawyers globally and more than 130 attorneys in North America focused on employment law. A recent BTI Consulting survey of corporate counsel named Baker McKenzie a "standout" law firm for complex employment litigation. In addition, Chambers Global has recognized the Firm's employment practice with a Band 1 ranking for eight consecutive years.