Functional Area 06
Risk Management and Compliance

GLOBAL PROFESSIONAL IN HUMAN RESOURCES (GPHR)

2021 EDITION

Global Professional in Human Resources (GPHR) Workbook

Module Six: Risk Management and Compliance

2021 Edition

Table of Content

Introduction iii
Table of Content iv
Part One: Risk Management and Compliance 6
1. HR Risk Management 6
2. Risk for International Assignment 7
2.1. Safety and Security Risks 8
2.2. Health and Medical Risks 9
2.3. Legal Prosecution Risk 9
3. Emergency Planning for Expatriates 10
3.1. Assessing Risk 11
3.2. Building a Framework for an Emergency Plan 12
3.3. Putting Together an Evacuation Plan 14
3.4. Working with the Right Service Providers 14
3.5. An Anecdote with a Moral 15
3.6. Starting on the Right Foot 15
3.7. Preparedness and Response 17
4. Extraterritorial Laws 17
4.1. U.S. Title VII of the Civil Rights Act 18
4.2. U.S. Americans with Disabilities Act (ADA) 18
4.3. U.S. Foreign Corrupt Practices Act (FCPA) 18
4.4. UK Bribery Act 19
5. Employee Records and Data 19
5.1. The General Data Protection Regulation (GDPR) 20
5.2. EU Safe Harbor 25
5.3. Health Insurance Portability and Accountability Act (HIPAA) 39
5.4. Australian Privacy Principles (APPs) 42
6. Global HR Compliance 44
6.1. Assemble the compliance team 44
6.2. Articulate audit context and scope 45
6.3. Create a master audit checklist template 45
6.4. Align local-country checklists off the master 46
6.5. Conduct the audit 46
6.6. Report and implement remedial measures 47
7. Global employee investigation plan 47
7.1. Take Necessary Immediate Action 48
7.2. Review applicable policies 48

7.3. Identify Investigator(s) 49
7.4. Assess special legal or cultural considerations 49
7.5. Develop An Interview Strategy 50
7.6. Preserve Evidence 50
7.7. Remediation across borders 51
Reference 53

Part One: Risk Management and Compliance

1. HR Risk Management

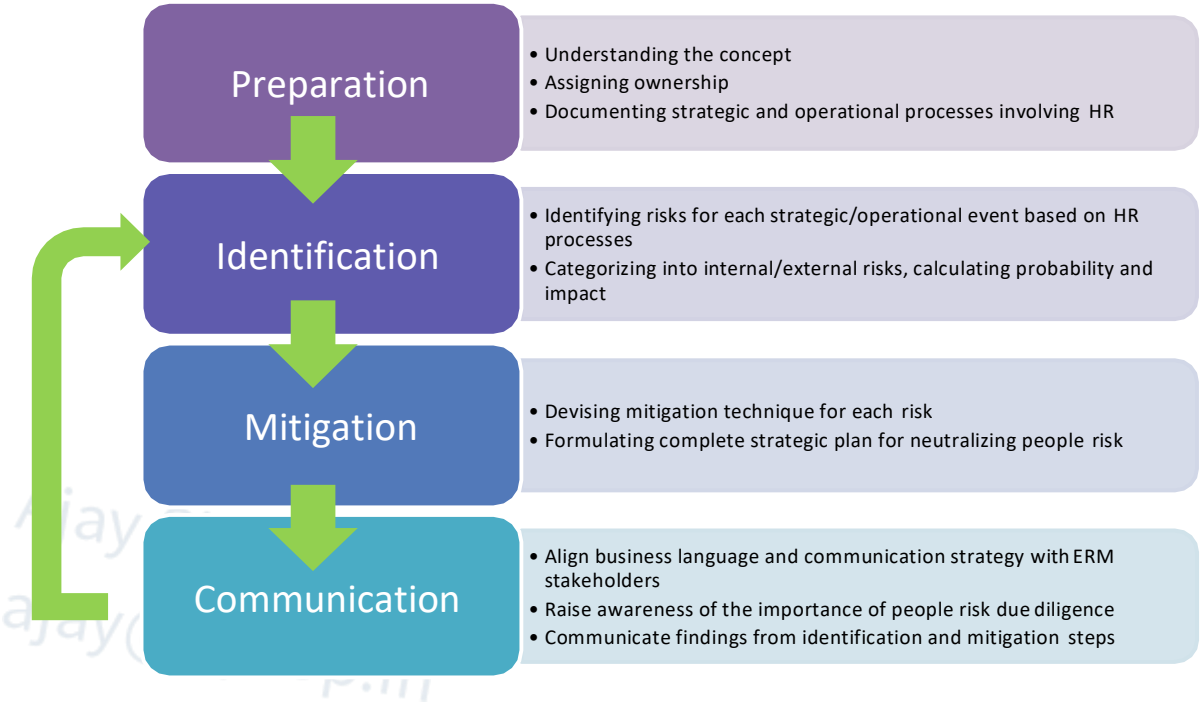
Research from global independent organizations shows that risk related to human resource management (”People Risk”) is largely ignored or misunderstood by HR and strategic-level planners. Furthermore, People Risk does not commonly feature as part of Enterprise Risk Management (ERM). A study by the Economist Intelligence Unit highlighted risk associated with human resource management as the most significant threat to global business operations. Another study by the Conference Board classified this risk as the fourth biggest impact on business performance, but placed it tenth in terms of how effectively it is measured and managed within the business.

By including the assessment of People Risk in regular HR planning activities, relevant stakeholders can recognize its significance and potential impact and then determine the necessary steps to mitigate those risks.

With the size and scope of People Risk, it’s important to get a clear understanding of the various elements that sit under this concept and place them in a structure that allows a business to include People Risk as an integral part of their risk management strategy.

The below figure illustrates a four-step process that Aon Hewitt has developed to allow HR professionals and related stakeholders to begin implementing a review of People Risk within their daily operations. The first step is for HR to prepare to handle People Risk by aligning its processes and language with the other types of risk that are already managed within the business. The second step is to identify People Risks based on the operational processes and strategic decisions in which the business partakes. The third step is to devise a strategy to minimize the impact of each risk on the business. Lastly, the fourth step is to communicate your findings to the risk management stakeholders within the organization and to ensure that HR is covered for the consequences of risk.

HR Process for Including People Risk as Part of the Company's Enterprise Risk Management Strategy



Source: Wade, G. (2012). Understand People Risk from Holistic Perspective. Aon Hewitt.

Once this is done, HR can return to identifying and monitoring risks as they appear. The following pages flesh out each stage of the diagram in detail.

2. Risk for International Assignment

In most large firms, even though responsibility for employee health and safety resides in the HR department, the HR manager responsible for international HR in the headquarters of an MNE does not often deal with health and safety issues among foreign subsidiaries or joint ventures. Responsibility for health and safety issues is normally left to the local subsidiary.

Additional areas of concern to multinational international HR managers within this topic of employee safety include the differences in medical systems in various countries (both in the form and quality of the delivery of medical services and in access to high-quality health care); the coverage of the health care system in different countries and who pays for health care; and the form and level of support systems for various forms of disabilities.

Expats or business travelers may be exposed to both health and safety risks. To identify risk areas, companies can check medical and political risk mappings. They can also take a look at the recommendations and advice provided by various institutions or government departments. Calling upon the services of a risk management specialist also is an option.

2.1. Safety and Security Risks

2.1.1. Terrorism

One aspect of the topic of health and safety for international HRM that has received a small amount of attention, but is probably the least important (unless, of course, it happens to you!), is the problem of terrorism and/or kidnapping (the subject of a separate heading). International terrorists have at times targeted the facilities and executives of MNEs (and/or their families). Even though the news media attention to these acts when they occur makes it seem as though they happen all the time, everywhere, to all expatriates and their families, the frequency of and danger involved with terrorist acts demonstrates that people are more likely to drown in their own bathtubs than to be killed by terrorists! This is not to say that expatriates and their families don't need to be briefed on such concerns and oriented to a constant awareness of the potential risks.

Of course, some countries present greater risks than others. And when expatriates are being asked to serve in locales of greater risk, greater precautions need to be taken. Various corporate reactions have ranged from essentially trying to ignore such terrorism to abandoning certain markets where such terrorism is seen as more likely. Some firms have tried to protect their managers and their families in various ways, such as fortifying their homes, providing trained chauffeurs and guards, and using local-sounding names for their subsidiaries to try to hide the identities of the MNE parents of their local operations. In addition, some firms have purchased kidnap and other kinds of insurance to cover their key executives.

2.1.2. Crime

Actually, the biggest threat to international travelers is not terrorism but old-fashioned crime, such as theft and pick-pocketing. In addition, the arrest and incarceration of traveling employees who either knowingly or innocently break local laws can be a major concern. "Travelers have been thrown in jail for exceeding a credit card limit, buying artifacts from an unlicensed dealer, entering an Islamic country with alcohol, or failing to meet a contract deadline." Indeed, in some countries, even false arrest of American personnel can be a problem, particularly where this is a practice of local, low-paid government officers or police to earn extra income.

And, then, while some expatriates end up in jail because they unknowingly commit what may seem (at least in their home countries) not very serious crimes, others may commit quite serious crimes while on foreign assignment (such as extortion or drug

trafficking). And yet others get involved with less serious but still quite illegal activities, such as drug and alcohol use, use of illegal prostitution, taking illegal pictures, or black market money exchange.

Here, as with the other areas described, international HR needs to prepare policies and procedures for dealing with such contingencies. And it needs to brief IAs and families on the seriousness of local law and how to access the support that the employer can provide.

2.1.3. Kidnapping

For international HR this poses a significant issue that must be addressed. Employee advising, special kidnap insurance, security for international assignment living quarters and for foreign offices and plants, special trained drivers, response plans, etc., all need to be addressed ahead of time by international HR. For any MNE with employees traveling to or residing in a country where there is a risk of terrorism, extortion, or kidnapping, IHR needs to do a thorough analysis of the risk and to employ security professionals to provide security briefings and protection for executives and other employees traveling to and/or residing in high risk cities and countries.

2.2. Health and Medical Risks

Business travelers and international assignees and their families frequently (if not usually) suffer from health complaints ranging from intestinal disorders due to exposure to new bacteria that the immune system is not used to major exotic illnesses.

The fear of ending up in situations where the sufficient level of medical care is not available can spoil any expatriation, journey or holiday. Language barriers, cultural differences, poor medical facilities or bad infrastructure can make expatriates feel uncomfortable and unsafe. The lack of cooperation between medical and social organizations excludes homeless people from medical care, and prevents health professionals from providing follow-up care, resulting in chronic diseases that may lead to recurring emergencies. MNCs can outsource these activities to vendors that provide specific health advice and customized medical kits based on health risk assessments for expatriates.

2.3. Legal Prosecution Risk

International assignees should be aware that the criminal prosecution process varies from one country to the next. They and their family members should know how to

request immediate assistance from the nearest consular office or embassy in the event of an arrest. A consular or embassy representative will explain the local judicial system; provide a list of local attorneys; contact family and friends (if authorized by the prisoner); facilitate the transfer of money, food, and clothing; ensure that the prison conditions are humane and healthy; arrange medical examinations, if appropriate; and protect against discriminatory treatment. Risk management begins with a clear understanding of the existing laws. While the other actions may help, knowledge of the law is most critical and is the logical place to begin.

Many firms find it important to retain one or more of the travelers' assistance programs or insurance programs that can provide help when the firm's overseas travelers or expatriates and their families experience difficul ties.

3. Emergency Planning for Expatriates

Due to political and social unrest in many areas of the world, employers must be prepared to bring international assignees and their family's home if their safety is threatened. Many global firms establish a corporate crisis team to create evacuation plans and make critical decisions during emergency situations.

Further, in the event of serious illness or injury without adequate hospital or medical facilities, civil strife, war, or similar emergencies in the host country, a Company may deem it necessary to evacuate the expatriate and accompanying dependents to another location. In such circumstances, the company may outsource a security institution to provide services including site surveys and security risk assessment, traveler education and advice, emergency response planning and security evacuation, crisis management services, security consultancy, site management, and staffing and training services.

The following texts provide helpful hints on what defines a cri sis location or situation, what issues need to be considered, and offers a framework for "constructing" an emergency plan.

Emergency Planning Process

Source: Dwyer, T. (2001). Take a Proactive, Rather than Reactive, Approach to Emergency Planning for Expatriates in Crisis Locations. KPMG.

3.1. Assessing Risk

Given the negative impact that the label "high risk" could have on inward investment and tourism, political, economic, or social factors sometimes prevent governments or their representatives from being completely candid about the degree of risk in certain locations. Therefore, it is important to establish valid criteria for determining when a location has become, or has the potential to become, high-risk. These factors can be used to supplement home- and host-government information to provide a comprehensive assessment of the host location. Such criteria could include:

- Anti-multinational/anti-"foreigner" demonstrations and/or riots;
- Rapid deterioration of the local economic or political environment;
- Threats from local political, religious, social, and other leaders;
- Evidence that military action may take place in the host country or a neighboring country;

- History of incidents against foreigners during volatile times;
- Known risk of natural disasters (such as earthquakes, typhoons, floods, etc.).

It is important not only to establish criteria, but also to effectively monitor them. Fortunately, the Internet has made this part of the job much easier, but it can still be time-consuming for hard-pressed HR professionals. Many rely on outside service providers for ongoing, updated risk assessments, which can help companies to make more informed decisions about their business strategies — those currently in place, and future — and, more importantly, evaluate the need to address real risks to their employees, whether at home or abroad.

Companies can also use this information to determine when to move to the next stage of their emergency plans, and to make sure that the company takes appropriate action, thereby precluding (potentially costly) premature or unnecessary action.

3.2. Building a Framework for an Emergency Plan

Any workable emergency plan must be location-specific, and must address a wide range of contingencies, incorporating both natural and man-made problems. However, it is possible to identify certain "best practice" elements which should be incorporated into all of them.

One thing most of these situations have in common is that there tends to be levels or stages of a crisis, from the initial indications of disquiet to the full-fledged "storm." Establishing a phased approach to emergency planning allows the company to avoid an "all or nothing" response. An example of the way in which a phased plan might be structured is set out below.

3.2.1. Stage 1: Warning

Your organization concludes that there is a greater-than-normal risk to your expatriate population; perhaps the political climate is unstable, religious or social leaders are stirring up anti-foreigner sentiment, or public demonstrations are larger and angrier than usual. In this case, the following steps can be taken:

- A "warning" is communicated to all expatriates, urging them to be more aware of their personal security and surroundings, and reminding them of emergency/evacuation procedures;
- A full employee/dependent census is taken;

- In-country travel by expatriates and dependents is strictly limited and tracked by local HR;
- Relevant embassies and consulates are contacted for advice and information specific to certain nationalities;
- New assignments to the host location are delayed and more carefully scrutinized for justification;
- Emergency/evacuation arrangements are confirmed with all vendors (transportation charter companies, security agencies, hotels, etc.).

3.2.2. Stage 2: Imminent Danger

At this point, it is clear that the risks to your employees have risen to the point where the employees may be in imminent physical danger. There might be serious doubts about the viability of political structures, people are being injured or killed in riots, and there is no longer real confidence that local police will be able to control the situation. Some of the steps at this stage might be:

- Evacuation of all dependents;
- Cancellation of all travel within the country, as well as of all new assignments;
- A review is conducted to ascertain if any segment of the local employee population is in possible need of assistance, for reasons of religion, ethnicity, or some other factor;
- Planning should take place (and procedures agreed and appropriately communicated) so that if a total evacuation of expatriates is necessary, local operations can be administered by "skeleton staffs" of non-expatriate personnel, or perhaps long-distance from neighboring countries.

3.2.3. Stage 3: Crisis

Civil order has now disintegrated, perhaps the government has collapsed, military action might be taking place, and given the risks, there is no business justification for keeping expatriates in the country. Steps would include:

- Full evacuation according to pre-agreed procedures, of expatriate and "at-risk local" population;
- Shut down of operations, or administration by local staff;

- Confirmation of census to ensure that no one is left behind.

It is important to note that the steps outlined above represent only guidelines. Each plan should be adapted to the particular company and its expatriate population, and to each specific host location and its circumstances. Internal and external experts should review plans.

3.3. Putting Together an Evacuation Plan

An evacuation plan can be looked at as a subset of an emergency plan. While it is hoped that an evacuation plan will never be used, it is absolutely essential to the health and safety of your expatriate population. Much more than the sample outline of the emergency plan above, an evacuation plan must be: location-specific; detailed; familiar to every expatriate and all local management; and operational under the assumption that much of the location's infrastructure (phone lines, cell phone towers, Internet access, airports, etc.) will not be functioning.

Of course, the formulation of this plan ought to be driven by local expertise whenever available — no amount of long-distance research can replace local insight. A wide variety of emergencies may cause an evacuation. In some instances you may have a day or two to prepare, while other situations might call for an immediate evacuation. Planning ahead is vital to ensuring that you can evacuate quickly and safely, no matter what the circumstances.

3.4. Working with the Right Service Providers

Many of the crucial steps involved in safeguarding expatriates, from the gathering and analysis of information and providing added security to the physical evacuation, are heavily dependent upon external service providers who will be available where and when needed. Among the types of organizations which might play a role are:

- Informational/risk assessment organizations;
- Cross-cultural/counseling/employee assistance programs;
- Medical evacuation services;
- HRIS vendors to help accurately track populations and their whereabouts;
- Locally-based security firms to provide added protection to your personnel and facilities;
- Insurance vendors to augment medical and life coverage as necessary;

- Transportation companies, including bus, plane, boat, or car services;
- Hotels and/or other logical canvassing points.

The organization must determine, for each of these providers, the timing and scope of services. It is crucial to remember that, by definition, the times when these services are to be provided will be unusual and often difficult. Therefore, it is not enough to know how the service providers operate when things are calm or during business hours, but instead how good they are at "keeping their heads while all about them are losing theirs."

3.5. An Anecdote with a Moral

In the early 1990's, during a particularly violent period in one South American country, an expatriate challenged his employer's assertion (based on State Department data) that the assignment location in question did not merit a danger premium. The expatriate argued that he and his family felt in danger of kidnapping, that many in the expatriate community had been subject to assaults and threats, and he did not even feel safe in his home. Surely, this was what a danger premium was designed to address. The employer offered to move the employee to more secure housing with gates and 24-hour guard protection. The employee refused, saying that his current home was very comfortable, and the location was convenient to the office. The company also offered to provide a security guard/driver to take his children to school and accompany his wife on her errands. This, too, the employee refused, explaining that his wife liked her freedom and flexibility, and a driver would be too constricting and intrusive. The company even offered to repatriate the employee ahead of schedule, but this option was also refused. However, he still wanted the money.

The "moral" of the story, of course, is that while an expatriate may be entirely justified in demanding additional pay for undertaking a potentially risky assignment, no amount of money itself can address the underlying goal of risk mitigation and personal safety for expatriates and their families. No one should be under the illusion that paying a danger premium provides any form of security. Taken in conjunction with other, practical steps, it may very well be good policy, but it is not a useful policy on its own.

3.6. Starting on the Right Foot

There are also some steps that individual expatriates and their employers can take which can lessen their chances of the expatriate coming into harm's way and, should something life-threatening occur, can protect the expatriate and his or her loved ones;

some of these are described below.

Certainly among the most practical steps is that the expatriate and family become familiar with the geography, and especially, the customs and laws of the assignment location. Doing so may lessen the chances that an unintentional infraction or offense will put the expatriate under a great degree of scrutiny or unnecessarily inflame an already-heated situation. Expatriates should also note local emergency numbers (e.g., a general "911"-type telephone number), and separately note the telephone numbers for the police, fire department, and medical services.

It is also crucial that the expatriate register with his or her home country's nearest embassy or consulate, and know to contact them immediately in case of trouble. The employee's own government can bring enormous legal, logistical, and financial resources to bear that can prove invaluable in "extracting" an expatriate from a tight spot.

It is also helpful if expatriate employees and their families make contacts with other expatriates, whether they are affiliated with the same employer or part of a broader expatriate community in the host location. Generally, these contacts and connections are useful in good times and, in bad, they can be extremely practical and valuable.

Recently, a company with only one expatriate in a high-risk location considered the possibility of evacuating that employee until the regional situation stabilized. Other organizations with expatriates in the region urged them not to, for fear that such a move would send a wave of panic through the expatriate community and be viewed by the locals as a vote of "no confidence" by the multinational community. Evacuation plans were temporarily put on hold.

Remarkably enough, when this company approached those same organizations to see if they would be willing to include this lone assignee in any future evacuation arrangements, the company was advised that, due to potential liability issues, evacuation assistance could not be extended to non-employees. Fortunately, this kind of situation is not common. In fact, during times of crisis, most multinationals exte nd an invaluable helping hand to each other. This is born partly of the camaraderie typically found among expatriates, which is especially strong in remote or difficult locations. From a public-relations standpoint, one is hard pressed to imagine any major company that would be willing to evacuate its own expatriates and leave those of other companies on the tarmac.

In areas where an organization does not have a large presence, much is to be gained by

working closely with other companies, even competitors. Such cooperation can range from sharing information to sharing charter planes, phone lines, and canvassing points.

Much is to be gained by ensuring that the expatriate is placed in reasonably secure housing. Arrangements will vary widely depending upon the situation in the host location, but can include secure compounds, "gated communities," buildings with 24-hour security, or even just a home with a good electronic system wired to the local police. This is an area where expatriates and their employers have sometimes been known to try to cut corners (secure housing can be expensive), but surely is an investment worth making.

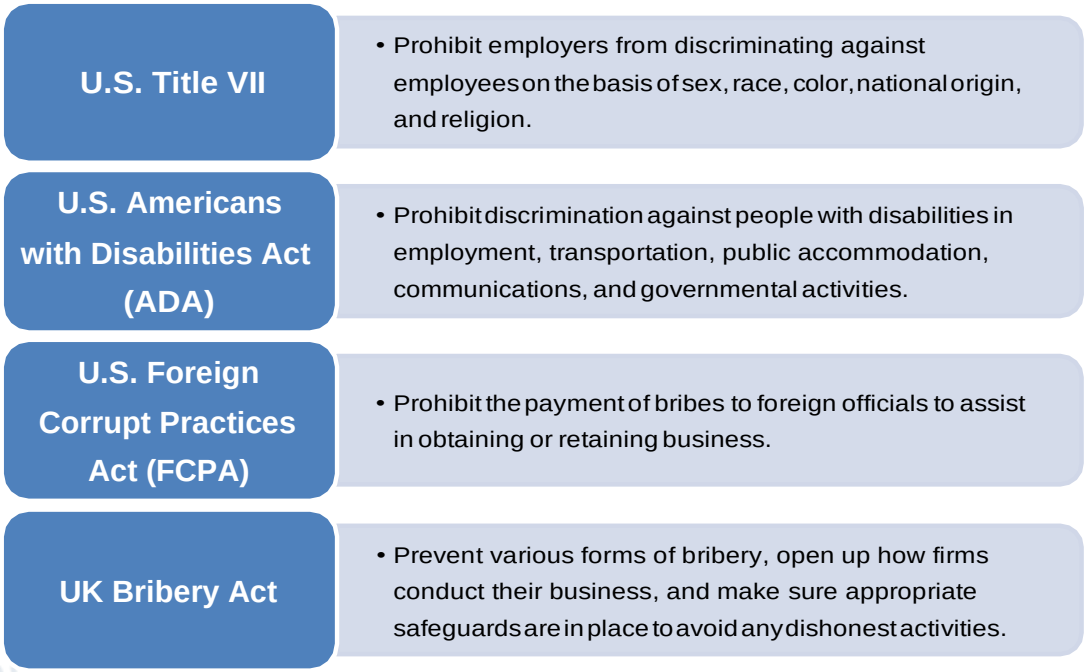
The additional complications can be time consuming, expensive, and emotionally taxing for the survivors. As much as we do not want to consider the possibility of employees dying while on assignment, the potential complications are great enough to warrant every company reimbursing a certain amount of estate planning, and strongly urging all of their expatriates to address the issue.

3.7. Preparedness and Response

As memories of the crisis passed, HR professionals' attention soon turned back to the time-consuming and difficult issues of expatriate pay and international taxation. It did not help that HR departments found budgets and resources slashed in the pursuit of greater corporate efficiency and increased shareholder value. It soon became apparent that the time, effort, and resources necessary to plan for future crises would just not be available. Many companies now find themselves again scrambling to make up for lost time.

4. Extraterritorial Laws

Doing business globally means more opportunities, but also entails greater risks. Develop a risk management plan is the first step for doing business globally. Global HR professionals must comply with extraterritorial laws to mitigate risk to the organization. Extraterritorial laws refer to laws that a country will enact which regard an offence committed abroad as an offence committed within its borders. Just as local employment laws apply only to those employees who work in the specific country, the U.S. employment laws generally apply only to those employees who work in the United States or its territories. There are a few exceptions though, as the following four major employment laws have some application abroad:



4.1. U.S. Title VII of the Civil Rights Act

Title VII, the United State (U.S.) federal law that prohibits most workplace harassment and discrimination, covers all private employers, state and local governments, and educational institutions with 15 or more employees. In addition to prohibiting discrimination against workers because of race, color, national origin, religion, and sex, those protections have been extended to include barring against discrimination on the basis of pregnancy, sex stereotyping, and sexual harassment of employees.

4.2. U.S. Americans with Disabilities Act (ADA)

Disability discrimination also occurs when a covered employer or other entity treats an applicant or employee less favorably because she has a history of a disability (such as cancer that is controlled or in remission) or because she is believed to have a physical or mental impairment that is not transitory (lasting or expected to last six months or less) and minor (even if she does not have such an impairment). The law requires an employer to provide reasonable accommodation to an employee or job applicant with a disability, unless doing so would cause significant difficulty or expense for the employer ("undue hardship").

4.3. U.S. Foreign Corrupt Practices Act (FCPA)

The Foreign Corrupt Practices Act was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government

officials to assist in obtaining or retaining business. Specifically, the anti -bribery provisions of the FCPA prohibit the willful use of the mails or any means of instrumentality of interstate commerce corruptly in furtherance of any offer, payment, promise to pay, or authorization of the payment of money or anything of value to any person, while knowing that all or a portion of such money or thing of value will be offered, given or promised, directly or indirectly, to a foreign official to influence the foreign official in his or her official capacity, induce the foreign official to do or omit to do an act in violation of his or her lawful duty, or to secure any improper advantage in order to assist in obtaining or retaining business for or with, or directing business to, any person.

4.4. UK Bribery Act

The Bribery Act is an act of Parliament that has been implemented into United Kingdom (UK) law in order to not only prevent various forms and elements of bribery, but also to open up how firms conduct their business, and make sure appropriate safeguards are in place to avoid any dishonest activities. Bribery itself is defined as both the giving and receiving of bribes in terms of someone who facilitates, gives or receives an advantage (which is usually financial) in connection with a person performing a function improperly.

The Act was introduced in response to international pressure from the Organization for Economic Co-operation and Development (OECD) and in order to bring the UK in line with efforts in other countries, particularly the US.

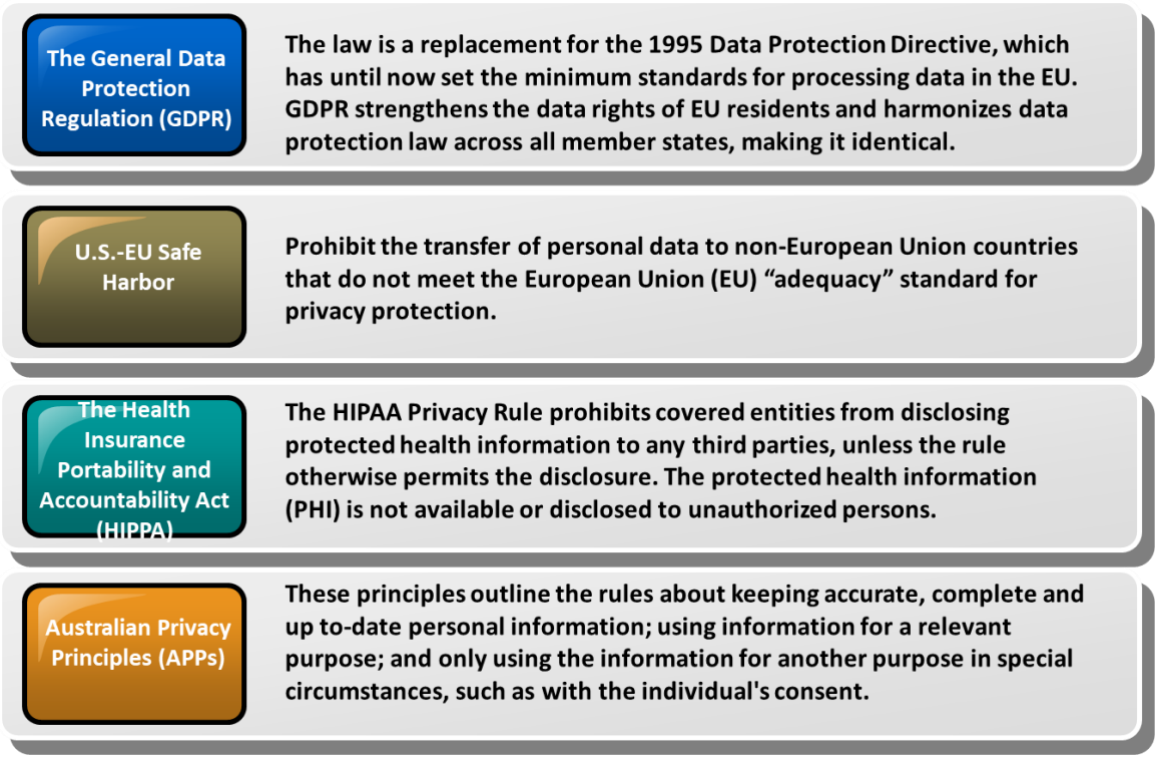
A company is under a positive duty under the act to ensure there are appropriate procedures in place to prevent bribery. If these procedures have been put in place then it is unlikely a company will be punished under the act; it is therefore extremely important that companies are aware of this and act accordingly. Another key point to note is that companies must continue to ensure that any hospitality offered to potential clients is both reasonable and proportionate.

5. Employee Records and Data

Employers collect a substantial amount of personal information about their employees. Companies need to be aware of their obligations under the profusion of data protection laws and regulations that govern the collection, use and transfer of personal information. This is an especially daunting task for companies that have operations subject to the laws of multiple jurisdictions, as requirements vary widely from country to country.

Companies use employees' personal information for a variety of purposes—from evaluating applicants during the hiring process to administering payroll and employee benefit plans to managing separation and other post-employment benefits. And as more employers adopt enterprise-level information management systems and outsource certain human resources administration functions, increasing amounts of personal data is being transferred and shared within and between organizations. Maintaining compliance with applicable data privacy laws is a responsibility employers cannot afford to overlook.

Many (but not all) data privacy laws exempt Personal Data that has been encrypted. Certain types of "Sensitive Data" are often given enhanced protection under comprehensive data protection regimes. Sensitive Data may include, for example, race, ethnicity or national origin, political opinions or associations, union membership, sexual orientation, marital status, health-related information and criminal history. It should be noted that data privacy laws are not restricted to protecting active employee information, so companies' obligations extend to any non-employee groups whose Personal Data they may acquire, such as clients and customers, but also job applicants, consultants, independent contractors and terminated or retired employees.



Employee Records and Data Protection

5.1. The General Data Protection Regulation (GDPR)

Whenever you open a bank account, join a social networking website or book a flight

online, you hand over vital personal information such as your name, address, and credit card number. What happens to this data? Could it fall into the wrong hands? What rights do you have regarding your personal information?

Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organizations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.

Every day within the EU, businesses, public authorities and individuals transfer vast amounts of personal data across borders. Conflicting data protection rules in different countries would disrupt international exchanges. Individuals might also be unwilling to transfer personal data abroad if they were uncertain about the level of protection in other countries.

Therefore, common EU rules have been established to ensure that your personal data enjoys a high standard of protection everywhere in the EU. You have the right to complain and obtain redress if your data is misused anywhere within the EU.

The General Data Protection Regulation (**GDPR**) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). The GDPR sets out the principles for data management and the rights of the individual, while also imposing fines that can be revenue-based. GDPR covers all companies that deal with data of EU citizens, so it is a critical regulation for corporate compliance officers at banks, insurers, and other financial companies. The law is a replacement for the 1995 Data Protection Directive, which has until now set the minimum standards for processing data in the EU. GDPR will significantly strengthen a number of rights: individuals will find themselves with more power to demand companies reveal or delete the personal data they hold; regulators will be able to work in concert across the EU for the first time, rather than having to launch separate actions in each jurisdiction; and their enforcement actions will have real teeth.

Even complying with the basic requirements for data access and deletion presents a large burden for some companies, which may not previously have had tools for collating all the data they hold on an individual.

But the largest impact will be on firms whose business models rely on acquiring and exploiting consumer data at scale. If companies rely on consent to process data, that consent now has to be explicit and informed – and renewed if the use changes. Under

the GDPR, individuals have:

5.1.1. The right to access

This means that individuals have the right to request access to their personal data and to ask how their data is used by the company after it has been gathered. The company must provide a copy of the personal data, free of charge and in electronic format if requested.

5.1.2. The right to be forgotten

If consumers are no longer customers, or if they withdraw their consent from a company to use their personal data, then they have the right to have their data deleted.

5.1.3. The right to data portability

Individuals have a right to transfer their data from one service provider to another. And it must happen in a commonly used and machine readable format.

5.1.4. The right to be informed

This covers any gathering of data by companies, and individuals must be informed before data is gathered. Consumers have to opt in for their data to be gathered, and consent must be freely given rather than implied.

5.1.5. The right to have information corrected

This ensures that individuals can have their data updated if it is out of date or incomplete or incorrect.

5.1.6. The right to restrict processing

Individuals can request that their data is not used for processing. Their record can remain in place, but not be used.

5.1.7. The right to object

This includes the right of individuals to stop the processing of their data for direct marketing. There are no exemptions to this rule, and any processing must stop as soon as the request is received. In addition, this right must be made clear to individuals at the very start of any communication.

5.1.8. The right to be notified

If there has been a data breach which compromises an individual's personal data, the individual has a right to be informed within 72 hours of first having become aware of the breach.

The GDPR is the EU's way of giving individuals, prospects, customers, contractors and employees more power over their data and less power to the organizations that collect and use such data for monetary gain.

Accordingly, a global company must respect key principles when processing personal data, such as:

- Fair and lawful processing
  - ✓ Lawful means all processing should be based on a legitimate purpose.
  - ✓ Fair means companies take responsibility and do not process data for any purpose other than the legitimate purposes.
  - ✓ Transparent means that companies must inform data subjects about the processing activities on their personal data.
- Data minimization

  "Data minimization" refers to measures performed by organizations to limit the personal data they collect and process from individuals to include only information that is relevant or necessary to accomplish specific purposes. The companies are expected to limit the processing, collect only that data which is necessary, and not keep personal data once the processing purpose is completed. This would effectively bring the following requirements:

  - ✓ forbid processing of personal data outside the legitimate purpose for which the personal data was collected
  - ✓ mandate that no personal data, other than what is necessary, be requested
  - ✓ ask that personal data should be deleted once the legitimate purpose for which it was collected is fulfilled
- Data subject rights

  The data subjects have been assigned the right to ask the company what

information it has about them, and what the company does with this information. In addition, a data subject has the right to ask for correction, object to processing, lodge a complaint, or even ask for the deletion or transfer of his or her personal data.

- Consent

As and when the company has the intent to process personal data beyond the legitimate purpose for which that data was collected, a clear and explicit consent must be asked from the data subject. Once collected, this consent must be documented, and the data subject is allowed to withdraw his consent at any moment. Also, for the processing of children's data, GDPR requires explicit consent of the parents (or guardian) if the child's age is under 16.

- Personal data breaches

The organizations must maintain a Personal Data Breach Register and, based on severity, the regulator and data subject should be informed within 72 hours of identifying the breach.

- Privacy by Design

Companies should incorporate organizational and technical mechanisms to protect personal data in the design of new systems and processes; that is, privacy and protection aspects should be ensured by default.

- Data Protection Impact Assessment

To estimate the impact of changes or new actions, a Data Protection Impact Assessment should be conducted when initiating a new project, change, or product. The Data Protection Impact Assessment is a procedure that needs to be carried out when a significant change is introduced in the processing of personal data. This change could be a new process, or a change to an existing process that alters the way personal data is being processed.

- Data transfers

The controller of personal data has the accountability to ensure that personal data is protected and GDPR requirements respected, even if processing is being done by a third party. This means controllers have the obligation to ensure the protection and privacy of personal data when that data is being transferred

outside the company, to a third party and / or other entity within the same company.

- Data Protection Officer

When there is significant processing of personal data in an organization, the organization should assign a Data Protection Officer (DPO). When assigned, the Data Protection Officer would have the responsibility of advising the company about compliance with EU GDPR requirements.

- Awareness and training

Organizations must create awareness among employees about key GDPR requirements, and conduct regular trainings to ensure that employees remain aware of their responsibilities with regard to the protection of personal data and identification of personal data breaches as soon as possible.

5.2. EU Safe Harbor

US-EU Safe Harbor is a streamlined process for US companies to comply with the EU Directive on the protection of personal data. It requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection.

The Safe Harbor Principles are designed to prevent accidental information disclosure or loss. US companies can opt into the program as long as they adhere to the 7 principles and the 15 frequently asked questions and answers (FAQs) outlined in the Directive.

U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbor organizations, except where organizations have committed to cooperate with European Data Protection Authorities. Unless otherwise stated, all provisions of the Safe Harbor Principles and Frequently Asked Questions apply where they are relevant.

5.2.1. Safe Harbor Principles

Organizations must comply with the seven Safe Harbor principles. The principles require the following:

(1) Notice: Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which they disclose the information and the choices and means the organization offers for limiting its use and disclosure.

(2) Choice: Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

(3) Onward Transfer (Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the Safe Harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

(4) Access: Individuals must have access to personal information about themselves that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

(5) Security: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

(6) Data integrity: Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

(7) Enforcement: In order to ensure compliance with the Safe Harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the Safe Harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants and Safe-Harbor benefits will no longer be assured.

5.2.2. Frequently asked questions and answers

(1) *Must an* organization *always provide explicit (opt-in) choice with respect to sensitive data?*

No, such choice is not required where the processing is:

1. in the vital interests of the data subject or another person;

2. necessary for the establishment of legal claims or defenses;

3. required to provide medical care or diagnosis;

4. carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;

5. necessary to carry out the organization's obligations in the field of employment law; or

6. related to data that are manifestly made public by the individual.

(2) *Given U.S. constitutional* protections *for freedom of the press and the Directive's exemption for journalistic material, do the Safe Harbor Principles apply to personal information gathered, maintained, or disseminated for journalistic purposes?*

Where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Safe Harbor Principles.

(3) *Are Internet* service *providers (ISPs), telecommunications carriers, or other organizations liable under the Safe Harbor Principles when on behalf of another organization they merely transmit, route, switch or cache information that may violate their terms?*

No. As is the case with the Directive itself, the Safe Harbor does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.

(4) *The activities of auditors and investment bankers may involve processing personal data without the* consent *or knowledge of the individual. Under what circumstances is this permitted by the Notice, Choice, and Access Principles?*

Investment bankers or auditors may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of companies' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

(5) *How will companies that commit to cooperate with European Union Data Protection Authorities (DPAs)* make *those commitments and how will they be implemented?*

More specifically as set out in the Enforcement Principle, they must provide (a) recourse for individuals to whom the data relate, (b) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true, and (c) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a) and (c) of the Enforcement Principle if it adheres to the requirements of this FAQ for cooperating with the DPAs

(6) *How does an organization self-certify that it adheres to the Safe Harbor Principles?*

To self-certify for the Safe Harbor, *organizations* can provide to the Department of Commerce (or its designee) a letter – signed by a corporate officer on behalf of the organization that is joining the Safe Harbor.

(7) *How do organizations provide follow up procedures for verifying that the attestations and assertions they make about their Safe Harbor privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Safe Harbor Principles?*

To meet the verification *requirements* of the Enforcement Principle, an organization may verify such attestations and assertions either through self-assessment or outside compliance reviews.

Under the self- assessment *approach*, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible.

It would also need to indicate that its privacy policy conforms to the Safe Harbor Principles; that individuals are *informed* of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self- assessment should be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.

Organizations should retain their records on the implementation of their Safe Harbor

privacy practices and make them *available* upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction.

Where the organization has chosen outside compliance review, such a review needs to demonstrate that its privacy policy regarding personal information received from the EU conforms to the Safe Harbor Principles that it is being complied with and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include without limitation auditing, random reviews, use of "decoys," or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed should be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance.

(8) *Individuals must have access to personal information about them that an organization holds and be able to correct, amend or delete that information where it is inaccurate, except where the* burden *or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the legitimate rights of persons other than the individual would be violated.*

Question 1: *Is the right of access absolute?*

No. Under the Safe Harbor Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to *verify* the accuracy of information held about them. Nonetheless, the obligation of an organization to provide access to the personal information it holds about an individual is subject to the principle of proportionality or reasonableness and has to be tempered in certain instances. Indeed, the Explanatory Memorandum to the 1980 OECD Privacy Guidelines makes clear that an organization's access obligation is not absolute. It does not require the exceedingly thorough search mandated, for example, by a subpoena, nor does it require access to all the different forms in which the information may be maintained by the organization.

Rather, experience has shown that in responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for

the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with and/or about the nature of the information (or its use) that is the subject of the access request. Individuals do not, however, have to justify requests for access to their own data.

Expense and burden are important factors and should be taken into account but they are not controlling in determining whether providing access is reasonable. For example, if the information is used for decisions that will significantly affect the individual (e.g., the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these FAQs, the organization would have to disclose that information even if it is relatively difficult or expensive to provide.

If the information requested is not sensitive or not used for decisions that will significantly affect the individual (e.g., non-sensitive marketing data that is used to determine whether or not to send the individual a catalog), but is readily available and inexpensive to provide, an organization would have to provide access to factual information that the organization stores about the individual. The information concerned could include facts obtained from the individual, facts gathered in the course of a transaction, or facts obtained from others that pertain to the individual.

Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be denied in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

Question 2: *What is* confidential *commercialinformation and may organizations deny access in order to safeguard it?*

Confidential commercial information is information which an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. The particular computer program an organization uses, such as a modeling program, or the details of that program may be confidential commercial information. Where confidential commercial information can be readily separated from other information subject to an access request, the organization should redact the

confidential commercial information and make available the non-confidential information. Organizations may deny or limit access to the extent that granting it would reveal its own confidential commercial information as defined above, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another where such information is subject to a contractual obligation of confidentiality in circumstances where such an obligation of confidentiality would normally be undertaken or imposed.

Question 3: *In providing access, may an organization disclose to individuals personal information about them derived* from *its data bases or is access to the data base itself required?*

Access can be provided in the form of disclosure by an organization to the individual and does not require access by the individual to an organization's data base.

Question 4: *Does an* organization *have to restructure its data bases to be able to provide access?*

Access needs to be provided only to the extent that an organization stores the information. The access principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

Question 5: *These replies make* clear *that access may be denied in certain circumstances. In what other circumstances may an organization deny individuals access to their personal information?*

Such circumstances are limited, and any reasons for denying access must be specific. An organization can refuse to provide access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:

a. interference with execution or enforcement of the law, including the prevention, investigation or detection of offenses or the right to a fair trial;

b. interference with private causes of action, including the prevention, investigation or detection of legal claims or the right to a fair trial;

c. disclosure of personal information pertaining to other individual(s) where such

references cannot be redacted;

d. breaching a legal or other professional privilege or obligation;

e. breaching the necessary confidentiality of future or ongoing negotiations, such as those involving the acquisition of publicly quoted companies;

f. prejudicing employee security investigations or grievance proceedings;

g. prejudicing the confidentiality that may be necessary for limited periods in connection with employee succession planning and corporate re-organizations; or

h. prejudicing the confidentiality that may be necessary in connection with monitoring, inspection or regulatory functions connected with sound economic or financial management; or

i. other circumstances in which the burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated.

An organization which claims an exception has the burden of demonstrating its applicability (as is normally the case). As noted above, the reasons for denying or limiting access and a contact point for further inquiries should be given to individuals.

Question 6: *Can an organization charge a fee to cover the cost of providing access?*

Yes. The OECD Guidelines recognize that organizations may charge a fee, provided that it is not excessive. Thus organizations may charge a reasonable fee for access. Charging a fee may be useful in discouraging repetitive and vexatious requests.

Organizations that are in *the* business of selling publicly available information may thus charge the organization's customary fee in responding to requests for access. Individuals may alternatively seek access to their information from the organization that originally compiled the data. Access may not be refused on cost grounds if the individual offers to pay the costs.

Question 7: *Is an organization required to provide access to personal information derived from public records?*

To clarify first, public records *are* those records kept by government agencies or entities at any level that are open to consultation by the public in general. It is not necessary to apply the Access Principle to such information as long as it is not

combined with other personal information, apart from when small amounts of non-public record information are used for indexing or organizing public record information. However, any conditions for consultation established by the relevant jurisdiction are to be respected. Where public record information is combined with other non-public record information (other than as specifically noted above), however, an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.

Question 8: *Does the Access Principle have to be applied to publicly available personal information?*

As with public record information (see Question 7), it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly *available* information.

Question 9: *How can an organization protect itself against repetitious or vexatious requests for access?*

An organization does not have to respond to *such* requests for access. For these reasons, organizations may charge a reasonable fee and may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.

Question 10: *How can an organization protect itself against fraudulent requests for access?*

An organization is not *required* to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.

Question 11: *Is there a time within which responses must be provided to access requests?*

Yes, organizations should respond without *excessive* delay and within a reasonable time period. This requirement may be satisfied in different ways as the explanatory memorandum to the 1980 OECD Privacy Guidelines states. For example, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests.

(9) *Human Resource*

Question 1: I*s the transfer from the EU to the United States of personal information collected in the context of the employment relationship covered by the Safe Harbor?*

Yes, where a company in the EU transfers personal information about its employees (past or present) collected in the context of *the* employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the Safe Harbor, the transfer enjoys the benefits of the Safe Harbor. In such cases, the coll ection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.

The Safe Harbor Principles are relevant only when individually identified records are transferred or accessed. Statistical reporting relying on aggregate employment data and/or the use of anonymized or pseudonymized data does not raise privacy concerns.

Question 2: *How do the Notice and Choice Principles apply to such information?*

A U.S. organization that has received employee information from the EU under the Safe Harbor may disclose it to third parties and/or use it for different purposes only in accordance with the Notice and *Choice* Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with choice before doing so, unless they have already authorized the use of the information for such purposes. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.

It should be noted that certain generally applicable conditions for transfer from some Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.

In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.

To the extent and for the period necessary to avoid prejudicing the legitimate interests of the organization in making promotions, appointments, or other similar employment

decisions, an organization does not need to offer notice and choice.

Question 3: *How does the Access* Principle apply?

The FAQs on access provide guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The Safe Harbor requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

Question 4: *How* will *enforcement be handled for employee data under the Safe Harbor Principles?*

In so far as information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the company in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employee works. This also includes cases where the alleged mishandling of their personal information has taken place in the United States, is the responsibility of the U.S. organization that has received the information from the employer and not of the employer and thus involves an alleged breach of the Safe Harbor Principles, rather than of national laws implementing the Directive. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.

A U.S. organization participating in the Safe Harbor that uses EU human resources data transferred from the Europe Union in the context of the employment relationship and that wishes such transfers to be covered by the Safe Harbor must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases. The DPAs that have agreed to cooperate in this way will notify the European Commission and the Department of Commerce. If a U.S. organization participating in the Safe Harbor wishes to transfer human resources data from a Member State where the DPA has not so agreed, the provisions of FAQ 5: The Role of the Data Protection Authorities will apply.

(10) *When data is transferred from* the *EU to the United States only for processing purposes, will a contract be required, regardless of participation by the processor in the Safe Harbor?*

Yes. Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU. The purpose of the contract is to protect the interests of the data controller, i.e. the person or body who dete rmines the purposes and means of processing, who retains full responsibility for the data vis-à-vis the individual(s) concerned. The contract thus specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure.

A U.S. organization participating in the Safe Harbor and receiving personal information from the EU merely for processing thus does not have to apply the Principles to this information, because the controller in the EU remains responsible for it vis-à-vis the individual in accordance with the relevant EU provisions (which may be more stringent than the equivalent Safe Harbor Principles).

Because adequate protection is provided by Safe Harbor participants, contracts with Safe Harbor participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the Member States) as would be required for contracts with recipients not participating in the Safe Harbor or otherwise not providing adequate protection.

(11) *How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organization's persistent failure to comply with the Principles be handled?*

The Enforcement Principle sets out the requirements for Safe Harbor enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ 7: Verification. This FAQ addresses points (a) and (c), both of which require independent recourse *mechanisms*. These mechanisms may take different forms, but they must meet the Enforcement Principle's requirements. Organizations may satisfy the requirements through the following: (1) compliance with private sector developed privacy programs that incorporate the Safe Harbor Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Union or their

authorized representatives. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle's requirements are additional to the requirement set forth in paragraph 3 of the introduction to the Principles that self- regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.

(12) *Does the Choice Principle permit an individual to exercise choice only at the beginning of a relationship or at any time?*

Generally, the purpose of *the* Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" (or choice) of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out." In the United States, individuals may be able to exercise this option through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.

Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if *the* organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.

(13) *When can airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, be transferred to organizations located outside the EU?*

Such information may be transferred in several different circumstances. Under Article 26 of the *Directive*, personal data may be transferred "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" on the condition that it (1) is necessary to provide the services requested by the consumer or

to fulfill the terms of an agreement, such as a "frequent flyer" agreement; or (2) has been unambiguously consented to by the consumer. U.S. organizations subscribing to the Safe Harbor provide adequate protection for personal data and may therefore receive data transfers from the EU without meeting those conditions or other conditions set out in Article 26 of the Directive. Since the Safe Harbor includes specific rules for sensitive information, such information (which may need to be collected, for example, in connection with customers' needs for physical assistance) may be included in transfers to Safe Harbor participants. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may inter alia impose special conditions for the handling of sensitive data.

(14) This FAQ is subject to Pharmaceutical and Medical Products. Those information are available on ec.europa.eu.

(15) *Is it necessary to apply* the *Notice, Choice and Onward Transfer Principles to public record information or publicly available information?*

It is not necessary to apply the Notice, Choice or Onward Transfer Principles to public record information, as long as it is not combined with non-public record information and as long as any conditions for consultation established by the relevant jurisdiction are respected.

Also, it is generally not necessary to apply the Notice, Choice or Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.

Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the Safe Harbor.

5.3. Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) offers protections for millions of American workers that improve portability and continuity of health insurance coverage.

After HIPAA went into effect, several sets of regulations were promulgated, two rules are key for marketers—the “Privacy Rule” and the “Security Rule”. The Privacy rule creates national standards to protect the privacy of personal information, while the Security Rule governs the security of electronic healthcare information. Each must be reviewed by organizations that are using health information of individuals.

The HIPAA Privacy Rule prohibits covered entities from disclosing protected health information to any third parties, unless the rule otherwise permits the disclosure. Some important issues are addressed as below:

5.3.1. Covered Entities

The Privacy Rule applies to “covered entities,” which are health plans, healthcare clearinghouses, and any healthcare provider who transmits health information in electronic form in connection with transactions. A “business associate” is a person or organization who is not employed by the covered entity who performs certain activities for a covered entity that involve the use or disclosure of individually identifiable health information.

5.3.2. Protected Health Information

The Privacy Rule applies to protected health information (PHI), which is individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media—electronic, paper, or oral. PHI includes demographic data; common identifiers (e.g., name, address, birth date, Social Security Number); information relating to the individual’s past, present, or future physical or mental health condition, healthcare provided to them, or payment for healthcare; and data that identifies the individual or that could be reasonably used to identify the individual.

5.3.3. Disclosures

A covered entity may not use or disclose PHI, except either as the Privacy Rule permits or requires, or as the individual who is the subject of the information (or the individual’s personal representative) authorizes in writing. Disclosure is required to be made to the individual/representative. A covered entity is permitted, but not required, to use and disclose PHI, without an individual’s authorization, for the following purposes or situations: (1) to the individual; (2) for treatment, payment, and healthcare activities like quality assessment or evaluations; (3) informal opportunities to agree or object such as providing information for hospital directories or notifications to family members; (4) disclosures incident to an otherwise permitted use and

disclosure; (5) public interest and benefit activities; and (6) the use or disclosure of limited data sets for the purposes of research, public health, or healthcare operations. Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

5.3.4. Disclosures for Public Interest and Benefit Activities

The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization, for a dozen enumerated public purposes. These disclosures are permitted, but not required, in recognition of the important uses made of health information beyond the realm of healthcare. Specific conditions or limitations apply to each public interest purpose.

5.3.5. Public Health Activities

Covered entities may disclose PHI to: (1) public health officials authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability; (2) public health or other government officials authorized to receive reports of child abuse and neglect; (3) entities subject to regulation regarding adverse event reporting, tracking of products, product recalls, and post-marketing surveillance; (4) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (5) employers requesting information regarding their employees for work-related illness or injury or workplace-related medical surveillance because the information is needed to comply with regulations.

5.3.6. Serious Threat to Health or Safety

The Privacy Rule allows covered entities to disclose PHI that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat).Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or criminal.

5.3.7. Judicial and Administrative Proceedings

The Privacy Rule permits covered entities to disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal.

5.4. Australian Privacy Principles (APPs)

The Privacy Act 1988 (Privacy Act) is an Australian law which regulates the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information, and access to and correction of that information.

The Australian Privacy Principles (APPs) regulate the handling of personal information by Australian government agencies and some private sector organizations.

5.4.1. Open and transparent management of personal information

The object of this principle is to ensure that APP entities manage personal information in an open and transparent way. An APP entity must have a clearly expressed and up to date policy (the APP privacy policy) about the management of personal information by the entity.

5.4.2. Anonymity and pseudonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

5.4.3. Collection of solicited personal information

An APP entity must not collect sensitive information about an individual unless the individual consents to the collection of the information.

5.4.4. Dealing with unsolicited personal information

The entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle if the entity had solicited the information.

5.4.5. Notification of the collection of personal information

At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must takes steps to notify the individual or to ensure that the individual is aware of any such matters.

5.4.6. Direct marketing

If an organization holds personal information about an individual, the organization must not use or disclose the information for the purpose of direct marketing despite

the individual has consented to the use or disclosure of the information for that purpose.

5.4.7. Cross-border disclosure of personal information

Before an APP entity discloses personal information about an individual to a person (the overseas recipient), the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to the information.

5.4.8. Adoption, use or disclosure of government related identifiers

An organization must not adopt a government related identifier of an individual as its own identifier of the individual unless the adoption of the government related identifier is required or authorized by or under an Australian law or a court/tribunal order.

5.4.9. Quality of personal information

An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

5.4.10. Security of personal information

If an APP entity holds personal information, the entity must take steps as are reasonable in the circumstances to protect the information. The entity must take steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

5.4.11. Access to personal information

If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

5.4.12. Correction of personal information

The entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is

held, the information is accurate, up to date, complete, relevant and not misleading.

6. Global HR Compliance

Cross-border HR compliance initiatives have many facets. A multinational has obvious incentives to verify that its overseas HR operations comply both with foreign local laws and with the growing list of "extraterritorial" laws that reach workplaces internationally. In addition to legal compliance, multinationals need to verify that their overseas operations conform to the organization's own in-house code of conduct, other international policies, employment agreements, and corporate values and norms.

This push for cross-border compliance assessments or audits of human resources operations can come from any of various constituencies within a multinational organization—for example, from compliance (of course), from upper management or the board of directors, from the general counsel's office, from human resources or from specific business functions—say, industrial safety (assessing global safety compliance), audit/accounting (assessing global Sarbanes-Oxley compliance), or mergers and acquisition teams (assessing employment compliance of to-be-spun-off or to-be-acquired business units). In fact, international HR employment compliance audits actually transcend employment law and become relevant to operations within an organization well beyond HR.

6.1. Assemble the compliance team

The first step in any global HR compliance check or audit is to assemble the compliance audit project team. In assembling that team, be sure to involve headquarters, foreign and local human resources staff, in-house legal and compliance functions and consider involving the corporate audit function. Consider tapping outside counsel with attorney/client privilege or at least involving an outside international HR consultant.

Audit team in place, the issue becomes global audit project management—how to manage this particular cross-border HR audit cost-effectively and efficiently. The temptation here can be the quick-and-dirty approach, grabbing some global HR audit checklist off the shelf, diving in and just doing the audit. Unfortunately, this approach never works because no one ever finds that one-size-fits-all "global HR audit checklist" that will serve as an accurate, sufficiently detailed roadmap for this particular project. That is because each global HR audit project spins off in its own uncharted direction, with its own specific goals, its own pool of affected countries and its own particular industry issues. Give up that search for the perfect off-the-shelf

global HR audit checklist. Instead, embrace the inevitable fact that your global HR compliance audit will require an organic approach.

6.2. Articulate audit context and scope

To begin any international human resources compliance check or audit, first isolate the context and delineate the scope of this particular audit project. Put aside all irrelevant, though auditable, issues not in play.

HR compliance assessments and audits arise in very different contexts including, for example, implementing a new corporate structure, preparing for a corporate restructuring, launching a merger or acquisition (spin-off or post-merger integration), responding to a lawsuit/government investigation, or simply toughening compliance through a robust HR practices check-up. Some global HR audits focus externally on outside supplier compliance while others focus internally on specific employment law challenges like health/safety, wage/hour, worker data privacy, whistle-blower hotlines, or—increasingly—corporate social responsibility and ethics. As mentioned, some HR-context audits actually focus on concerns separate from employment law, like compliance with bribery and insider trading laws.

After setting context, delineate audit project scope. Which countries are involved here? Should this global HR audit focus on compliance with laws, with collective agreements, with corporate policies, with best practices—or with all of these? As to legal compliance, should this audit look at local laws, at headquarters-country laws that reach extraterritorially—or both? Should this audit confine itself to local host-country employees, or should it also check expatriates, contingent staff, consultants, independent contractors and employees of suppliers? Should this audit go beyond employment laws and policies to assess compliance with HR-context data privacy, corporate and tax laws? And which industry-specific issues require special focus here (for example, wage/hour in retail, conflicts of interest/insider trading in financial and professional services, health/safety in manufacturing)?

6.3. Create a master audit checklist template

Compliance means following rules. Because HR-context rules differ significantly from jurisdiction to jurisdiction, anyone who leads a multijurisdictional compliance assessment or audit will need aligned but localized checklists or questionnaires that allow for “apples-to-apples” comparisons across jurisdictions. To align local HR audit checklists, first craft a single master global audit template or compliance checklist. Create that master template organically—tailor it to fit your particular audit project.

Include in your global audit template all topics consistent with the specific audit project scope and then actively exclude all other topics. By definition, topics outside the scope are irrelevant. Depending on context, topics possibly to include in a global HR compliance audit template or checklist might include:

- Local labor/employment laws and other laws reaching employees.
- Headquarters-country employment laws that reach overseas.
- Data privacy laws reaching employee data, personnel files and global Human Resources Information Systems.
- Past and pending employment claims/litigation.
- Benefits and compensation issues.
- Corporate, tax and other laws reaching employment.
- Written internal employment policies, rules and agreements.
- Individual employment contract issues.
- Collective (union/works council) agreements.
- Contingent and irregular staffing issues.

6.4. Align local-country checklists off the master

Next, localize the master HR audit checklist template by spinning it off into a set of tailored but aligned audit checklists, one per jurisdiction subject to the audit project, each anchored in the local legal standards. In addition to localizing topics from the master checklist for each affected jurisdiction, be sure to add into each local checklist all quirky local rules that, because they are inherently local, did not get picked up on the global template.

6.5. Conduct the audit

At last it becomes time to go out and conduct the global HR assessment or audit. Take the local checklists into the field and do the global HR compliance audit, gathering compliance information in each jurisdiction. Decide how the audit process will work and decide how deep to plow. Will headquarters auditors travel onsite—or can auditors conduct the field piece remotely or delegate local audits to local HR staff? Will auditors interview employees? Will auditor inspections be announced or surprise? How to handle local HR staff that fail to respond adequately? How to handle

the political issue of local management hostile to the audit? How to handle local staff refusing to cooperate? Under law in many jurisdictions, local staff does not have to cooperate. How granular will the audit be? Will auditors look only at policies/protocols/agreements? Or will auditors scrutinize specific employment agreements, employee-signed acknowledgements, minutes of union/works council meetings, paycheck stubs, timesheets, safety logs and the like? Will translations be needed? Will auditors get access to local outside providers like payroll agencies and benefits administrators? And how will the international audit process itself comply with local employment and data protection laws?

6.6. Report and implement remedial measures

Summarize the HR compliance audit findings. The summary report should avoid identifying specific employees (to minimize data protection and defamation exposure) and should account for attorney/client privilege and evidentiary admissions issues. Could the report later get used against the employer as evidence of willful noncompliance? Finally, the audit team should propose specific remedial measures, or fixes. Finally, someone needs to follow up to check that the fixes actually get implemented locally.

Source: Dowling, D. (2014). Auditing Global HR Compliance. www.shrm.org

7. Global employee investigation plan

The most common trigger of a cross border investigation is a lead or an allegation made

by an employee of the company. Almost half of these internal leads came through whistleblower and hotline programs, a notable figure given that cultures can differ widely regarding the acceptability of reporting the conduct of others.

In addition to cultural differences, the laws and regulations governing hotlines vary greatly from country to country. Data privacy laws in Europe, for instance, may restrict the use of whistleblower hotlines or even prohibit them from accepting anonymous calls. Some European Union countries require government approval or at least notification before establishing a hotline, while other countries compel companies to consult with employees and sometimes to get their consent before launching a hotline. Knowing the local culture and regulations about the triggers of cross-border investigations can help companies customize reporting channels to best fit the ways in which foreign employees might report allegations.

The importance of a prompt and thorough internal employee investigation is more evident than ever, and an effective investigation plan can protect the company's interests when reviewing internal complaints. Consider the following when developing an international investigation plan.

7.1. Take Necessary Immediate Action

When receiving a complaint, outline the issues involved to determine if there are any necessary immediate action items. Should the company separate the employees involved (e.g., implement schedule changes or a leave of absence, with an eye toward avoiding negative action against the complainant)? Is there threat of imminent harm to an individual? Will the investigation be compromised if the company does not take immediate action?

7.2. Review applicable policies

Review applicable policies (e.g., harassment, work rules, progressive discipline) and company practices related to the outlined issues. Review personnel files and other documents to assess whether there is a history of improper conduct, similar complaints in the past, and information relating to motive or bias.

An important early step in the case-management of cross-border investigations is to alert key members of management that a potentially significant compliance allegation has been filed and that an investigation will be initiated. Depending on the nature of the matter, it may be appropriate to notify the country manager, the functional leader, the department head, or other members of local management. It is

important to keep the circle of trust small and to remind members of management about confidentiality and the integrity of the process.

7.3. Identify Investigator(s)

In a cross-border context, the investigative team also needs to take into account any jurisdictional differences that may impact the investigation, the information that can be collected, and the individuals who can be interviewed. Allegations vary in substance, severity, and priority. Therefore, a company should have a detailed procedure or protocol that outlines which department or individuals will bear responsibility for overseeing the investigation.

While the legal department would likely oversee investigations involving potential legal matters, human resources may oversee investigations related to employee-relations issues, theft, and physical security. Moreover, potentially significant compliance situations, including those that involve serious violations of domestic or foreign law, fraudulent financial reporting, or senior management would require direct board or audit committee oversight. These oversight groups should help establish the scope of the investigation, review the investigation plan, and ensure that adequate resources are available.

Individuals need not only to be experienced in investigative strategy and tactics, but they also must understand local law, language, and customs. Investigation teams who do not have local language skills may miss critical aspects of key documents or interviews conducted in local language.

Unlike domestic investigations, cross-border investigations oftentimes require specialized staffing that necessitates proactive planning. Companies can address gaps in resources by developing contingency plans for investigative personnel, such as designating experienced internal people from other regions to respond if necessary, and retaining outside local investigators to be on call when a situation arises.

7.4. Assess special legal or cultural considerations

Before a company launches an investigation, it should consult with in-house or external counsel familiar with the law of the relevant jurisdiction as to whether the investigation can be privileged or protected. In an international setting, local law also may limit the scope of the investigation. Investigators should be sure that the scope of their investigative plan includes a review of whether the subject violated local law. While it is not uncommon for many companies to predicate their global standards

and compliance policies on their domestic laws, cross-border investigators should also evaluate whether local law, too, has been violated. Many times, these laws are not in alignment.

7.5. Develop An Interview Strategy

At the onset, identify key witnesses, when and where to conduct each interview (off - site, in private, conference room), and prepare a list of questions for each interviewee. Reference the outline of issues to ensure questions are tailored to elicit critical information and details associated with each issue. Anticipate that the witness list may be subject to change as the interviews progress. If necessary, witnesses may also be taken out of order and questions may be modified.

Interviewing employees who are located in a foreign country raises unique legal and cultural issues that oftentimes are fraught with pitfalls. In many countries, employees have the right to refuse to cooperate with an employer-led investigation, even if they are not its target. Labor laws in many countries mandate that an employee representative or union committee be consulted before an employer may interview its own employees in an investigation.

One of the starkest differences between domestic and cross-border investigations is the requirement that companies in some countries have to inform their employees of procedural rights during the investigation and give them at least some degree of access to investigation materials that identify them. Employees also may have the right to have a lawyer or employee representative present at the interview.

Moreover, understanding local culture plays a pivotal role with interviewing employees in cross-border investigations. Language differences can pose problems at every stage in cross-border investigations, and they may be most acute when interviewing witnesses. Using investigators with local language skills, particularly those having the appropriate regional dialects, can be essential when interviewing witnesses. When different languages are involved, another area that poses a high risk is obtaining an accurate translation that could create significant misinterpretations of the reported facts

7.6. Preserve Evidence

Through the course of an investigation, key documents, files, audio and visual recordings may be identified. Take measures to preserve these sources of information as needed. In light of potential allegations of cyberbullying and harassment, ask an

employee if they are willing and able to provide a copy of any purported harassing or discriminatory on-line post or text message. Further, ask the employee to retain the information until otherwise informed. Document such a request in the investigation plan.

Preserving and collecting information relevant to an investigation is one of the most important steps in the investigative process. Foreign data privacy laws and regulations pose some of the greatest challenges to conducting cross-border investigations because of restrictions on the kinds of data that can be collected and transferred out of the jurisdiction. Many countries have enacted laws that place a high priority on protecting personal data, including establishing a fundamental legal right on the privacy of personal data, even if such data are contained on an employer's system or computer.

The data privacy laws of some countries may prohibit a company from reviewing certain data in a company's own files unless the data originally was obtained for investigatory purposes, which many times is not the case. One of the biggest hurdles is complying with limitations on collecting and reviewing data in a company's readily-accessible files, such as emails on the company's server, internet use records, documents on an employee's hard drive, and even hard copy documents in an employee's office. Unlike a common presumption in some countries that a company has the right to search data on company-owned systems and computers, the prevailing view in many foreign countries is that personal data is protected regardless of where it is stored. The company has to understand whether there are restrictions on taking data out of the local country.

Careful attention should be paid to the form and content of a report in a cross-border investigation. There may be advantages to providing only an oral report, but the labor laws in a particular jurisdiction may require a written report, especially if disciplinary action is taken. However, an investigation report may contain data that is restricted from being transferred out of a jurisdiction, such as names of individuals, financial information, or personal data. Therefore, the proper data export channels need to be established before providing a report (even a report in draft form) to management or directors outside of the country. These considerations apply likewise to reports and materials prepared by experts and consultants.

7.7. Remediation across borders

Taking remedial action can be an important determinant by regulators, both

domestic and foreign, in deciding to charge a company with a violation of a law or to reduce the size of a criminal fine or penalty that might be assessed. Remediation across borders, however, can create unsuspecting challenges. One of the first considerations is how to handle employees found to have engaged in wrongdoing. These employees may have different levels of culpability and may be located in jurisdictions with different legal or labor protections against adverse action.

Even if the evidence appears to implicate a person, the labor laws in some countries contain high standards that must be met in order to justify a termination for cause. Domestic and foreign regulators also may complicate matters by requesting that a company not terminate a culpable employee so that the regulator continues to have access to the employee. Even in this situation, a company should change the responsibilities of the affected employee to make sure he or she cannot repeat past misdeeds or be put in a position with a comparable level of authority, which could be interpreted as insufficient punishment.

Another key area of remediation is to adequately address the deficient, insufficient, or ineffective controls or procedures that allowed the misconduct to occur or to avoid being detected. In a multi-national company, these controls and procedures need to be examined not only in the affected location, but also wherever they exist globally, and they need to be remediated if necessary. While regulators may be impressed with the overall level of effort, they, along with management and directors, may insist on an interim fix to the controls that provides assurance that some remedial action is occurring while a longer term solution is being implemented. Keep in mind, however, that in some countries there may be limitations on the ability of an employer to make substantive changes to the work environment without consulting labor unions or workers' councils.

The timing of remedial action also is a consideration. Oftentimes, remediation can and should begin as soon as inadequate or compromised financial controls have been identified, even during the investigative fact finding.

Reference

- Aon Hewitt (2015). Trends in Global Employee Engagement. Available on www.aon.com.
- Ball, D., Geringer, M., Minor, M., & McNett, J. (2012). International Business: The Challenge of Global Competition (13th Edition), New York, NY, US: McGraw-Hill/Irwin.
- Bamber, G.J., Lansbury, R.D., & Wailes, N. (2010). International and Comparative Employment Relation (Fifth Edition), Thousand Oaks, CA, US: SAGE Publications.
- Barends, A. (2014). 5 steps to create impactful employee surveys. Available on www.effectory.com.
- Claus, L. (2011). Duty of Care and Travel Risk Management Global Benchmarking Study. Available on www.internationalsos.com.
- Crim, D. & Seijts, G. (2006). What Engages Employees the Most OR, the Ten Cs of Employee Engagement. Ivy Business Journal, March/April. Available on iveybusinessjournal.com.
- DeNardis, L. (2015). The Global War for Internet Governance. New Haven, Connecticut, US: Yale University Press.
- Dowling, D. (2014). Auditing Global HR Compliance. Available on www.shrm.org
- Dwyer, T. (2001). Take a Proactive, Rather than Reactive, Approach to Emergency Planning for Expatriates in Crisis Locations. Available on www.us.kpmg.com.
- European Union (2015). Employee Involvement - European Works Councils. Available on europa.eu.
- International Labour Organization (2004). The International Labour Organization's Fundamental Conventions. Available on www.ilo.org.
- International Labour Organization (1998). ILO Declaration on Fundamental Principles and Rights at Work. Available on www.ilo.org.
- Isaac, L. (2010). What is Industrial Relations? Available on www.leoisaac.com.
- KPMG International (2013). Cross-border investigations: Are you prepared for the challenge? Available on www.kpmg.com
- Organization for Economic Co-operation and Development (OECD), (2014). OECD

Guidelines Chapter 5: Employment and Industrial Relations. Available on www.oecd.org.

- Ready-A national public service advertising (PSA) campaign, (2014). Risk Assessment. Available on www.ready.gov.
- Reed, S.M. (2017). A Guide to the Human Resource Body of Knowledge (HRBoK). Hoboken, New Jersey: John Wiley & Son.
- Tarique, I., & Briscoe, D., & Schuler, R. (2015). International Human Resource Management: Policies and Practices for Multinational Enterprises; 5 edition, (Global HRM). New York (USA): Routledge.
- Wade, G. (2012). Understand People Risk from Holistic Perspective. Available on www.aon.com.
- Wild, J.J. & Wild, K.L. (2015). International Business: The Challenges of Globalization (8th Edition). New Jersey, US: Prentice Hall.