K&L GATES

MULTINATIONAL EMPLOYER MONTHLY

Presented as Part of Global Employer Solutions

April 2015

Author:

Donald C. Dowling, Jr.

don.dowling@klgates.com

+1.212.536.3914

Multinational Employer Monthly focuses on international HR management and compliance topics essential to the global operational needs of multinational companies.

It is presented as part of K&L Gates' Global Employer Solutions, a comprehensive cross-disciplinary team working collaboratively with clients to meet the challenges of an ever expanding global workforce

How to Conduct Internal Investigations Outside the United States

Think of a U.S.-headquartered multinational when it receives an allegation of serious misconduct at one of its overseas operations. Maybe the company whistleblower hotline just got a tip that a secretary in the Buenos Aires office is trading on inside information. Or maybe the U.S. Justice Department has just asked for information about the company's recent entertainment of a certain government official in Saudi Arabia. Or perhaps an executive at the Toronto office has been complaining to colleagues that the managing director for Canada is harassing her. These are the types of allegations that give rise to an American multinational deciding to initiate a cross-border investigation.

But investigating across borders can be complex, expensive and risky. How does an American-based organization that is accustomed to doing internal investigations domestically within the United States go about investigating some alleged infraction at an *overseas facility*?

The way we conduct internal investigations domestically within the United States is well understood. These days lots of lawyers, consultants, private investigators, forensic accountants and other professionals specialize in conducting internal corporate investigations. These investigations can get hugely expensive and drawn-out: One American personal care products company disclosed in an SEC filing that it had somehow spent *$247.3 million* on a single internal investigation.

High-profile internal investigations can get so expensive and time-consuming because the stakes are high when an allegation involves millions of dollars and serious charges like bribery, sabotage, embezzlement, tax fraud, insider trading, antitrust collusion, workplace violence, environmental crimes, audit/accounting fraud or conflicts of interests. But these huge internal investigations are the exception. Most corporate internal investigations are streamlined, fast and inexpensive. Investigations into low-stakes claims alleging petty theft, bullying, harassment, workplace accidents, vandalism or expense-account fraud usually get wrapped up quickly and fairly inexpensively, often without involving outside experts.

Even so, in this era of Sarbanes-Oxley, Dodd-Frank, compliance departments and close scrutiny into corporate ethics—plus heightened focus on harassment and bullying in the workplace—an internal investigation, whether complex or routine, needs to be done correctly. Where employee wrongdoing is uncovered, appropriate discipline should follow. Investigators, meanwhile, must avoid committing their own infractions while they investigate.

These issues get more complex when an investigation goes global. Border-crossing internal investigations are becoming increasingly common in today's interconnected world. Not only do American lawyers and investigators expert in "white collar" criminal law frequently help U.S. headquarters investigate "extraterritorial" charges under U.S. federal law, but there is the much more common scenario of an allegation of breach of local laws outside the United States. Internal investigations have now become routine among companies based in Australia, Canada, England and other common-law jurisdictions that have adopted American-style investigatory practices. In England, for example, "[i]t is important to carry out necessary investigations of potential disciplinary matters without unreasonable delay to establish the facts of the case." (ACAS *Code of Practice on Disciplinary and Grievance Procedures*, Mar. 2015 at ¶5) In fact, in some parts of the world conducting an internal investigation into a possible local violation is mandatory. For example, Austria's Supreme Court requires employers to investigate sex harassment complaints (Austria Supreme Court decision 9 ObA 131/11x, Nov. 26, 2012), as do statutes in Chile, Costa Rica, India, Japan, South Africa, Venezuela and elsewhere. The British Columbia Worker's Compensation Act requires employers to conduct immediate investigations into workplace accidents that require medical treatment, as do other workplace safety laws. And workplace discrimination investigations are mandatory in Ontario, at least in situations where discrimination is later held to have actually occurred. (*Scaduto v. Ins. Search Bureau*, Human Rights Tribunal of Ontario [HRTO] Feb. 24, 2014 at ¶¶ 78,79,82; *Sears v. Honda of Canada*, HRTO Jan. 13, 2014 at ¶161; *Morgan v. Herman Miller Canada*, HRTO Apr. 18, 2013 at ¶ 95; *Ibrahim v. Hilton Toronto*, HRTO Apr. 22, 2013 ¶¶ 111,113)

Recent upticks in international criminal and civil enforcement have convinced multinationals of the need to do thorough border-crossing internal investigations. A U.S. multinational headquarters launching a cross-border or overseas local internal investigation may, by default, want to export its sophisticated tool kit of American investigatory strategies. U.S. companies see American investigatory techniques as vital in defending against a border-crossing criminal prosecution or civil lawsuit like a charge under the Foreign Corrupt Practices Act, terrorism financing rules, trade sanction laws, the Alien Tort Claims statute, international-context claims under Sarbanes-Oxley and Dodd-Frank, extraterritorial provisions of U.S. discrimination laws or even the UK Bribery Act 2010 (which might reach U.S.-based employers). Recent conferences, articles and even some books explicate many of the domestic American legal doctrines that can reach cross-border investigations. Common themes include:

- Contrasts between the U.S. Foreign Corrupt Practices Act and the UK Bribery Act 2010
- Overseas whistleblower denunciations under the U.S. Dodd-Frank whistleblower "bounty" program and the extraterritorial reach of U.S. Sarbanes-Oxley §301 hotline ("report procedure") provisions
- The effect of foreign "blocking statutes" and foreign data protection laws on U.S. litigation e-discovery
- Attorney-client privilege abroad as contrasted with the privilege in the United States
- U.S. bank secrecy laws in the international context
- "Suspicious activity reports" of infractions committed abroad and "self-reporting" to American government agencies
- U.S. "deferred prosecution" and "non-prosecution" agreements in the cross-border context
- Prosecutorial cooperation among enforcement authorities, parallel criminal proceedings in foreign jurisdictions and cross-jurisdictional settlements of criminal charges
- Credit for foreign corporate compliance programs under U.S. criminal sentencing guidelines

Any of these American "white collar" law issues might prove vital when investigating cross-border charges that implicate American criminal or civil laws and litigation, although of course these particular U.S. law issues tend not to arise when investigating foreign (outside-U.S.) local allegations with no U.S. exposure.

But all overseas internal investigations, whether they implicate these U.S. domestic law issues or not, simultaneously trigger completely different compliance challenges under the *foreign law of the workplace*. It is these foreign workplace law issues that impact cross-border investigations on which we focus here.

American multinationals exporting their American investigatory tool kits for overseas investigations run into problems abroad because American investigatory tools were forged in the uniquely American environment of *employment-at-will*. The law of the American workplace imposes fairly few constraints on how American employers have to investigate allegations of employee wrongdoing (*Weingarten* rights and *Upjohn* warnings aside, below ¶¶ 21,23). But overseas, especially in Europe, the regulatory environment differs greatly. Even in jurisdictions like Brazil that do not specifically regulate internal investigations, local data protection and employment laws can spring up and have profound effects on an internal investigation. As one American lawyer has noted, "some countries are not used to the 'American style' of investigations. They are quite interested in protecting their privacy and employment rules of the workplace." (*Quoted in* S. Russell-Kraft, "How to Avoid Botching Your Internal Investigations," Law 360, May 22, 2014) An in-house lawyer at a major American multinational told an American Bar Association conference in Atlanta on November 1, 2012: "One of the biggest mistakes an investigator can bring to a foreign investigation is an American mindset."

Any multinational launching either a border-crossing internal investigation or a foreign local investigation at an overseas location needs to retool American-forged investigatory practices for the radically different legal, cultural and workplace environment abroad. Because so many foreign laws that reach internal investigations have no counterparts under American employment-at-will, these rules may catch American investigators off-guard. Therefore, investigators based overseas can actually wield an advantage over their American counterparts. A London solicitor addressing American lawyers about internal investigations outside the United States has explained:

> "Most corporations that have faced a significant [international] investigation will be familiar with the need to balance the thoroughness of the investigation with the need to respect the [overseas] suspect's and the informant's data protection rights. Increasingly we are seeing [overseas employee] suspects and their advisors seek to exercise these rights to slow down or halt an investigation [outside the United States]. In at least one case where I have been involved, injunction proceedings were threatened [to stop the U.S.-driven internal investigation]." (J.P. Armstrong, "Anti-Corruption and Bribery Compliance: The U.K. Perspective," NY State Bar Intl Chapter News, Fall 2012 at 5, 9-10)

Of course, having to retrofit American-forged investigatory tools for more regulated overseas workplaces can frustrate American investigators who are naturally reluctant to tamper with proven investigation strategies and justifiably resistant to compromising investigatory best practices. But failing to modify American investigatory practices overseas can have serious consequences if investigators fail to follow local laws that regulate internal investigations.

Here is a 30-point checklist for American-headquartered multinationals that want to adapt their domestic American investigatory tools for cross-border and for overseas local internal investigations. The starting point in our discussion is the assumption that American companies value their American-style investigatory practices and prefer to export them for overseas investigations, modifying them only as necessary under local law. And so the 30 points we discuss here track the four stages of any thorough American-style internal investigation:

A. Launching an Investigation Protocol or Framework
B. Responding Initially to a Suspicion or Allegation Arising Abroad
C. Interviewing Witnesses Abroad
D. Discipline, Remedial Measures and Post-Investigatory Communications in Cross-Border Investigations

A. Launching an International Investigation Protocol or Framework

Americans like flexibility. When it comes to their investigatory practices, American multinationals are reluctant to lock themselves into formal protocols or frameworks that mandate specific steps for how they would have to conduct any given internal investigation. But overseas, crafting an investigation protocol or framework before an investigation is required can be helpful for a number of reasons. To pave the way for future internal investigations, take some steps to empower overseas investigation teams that will later look into suspicions or allegations of wrongdoing. Build an investigatory protocol or framework to facilitate a rapid headquarters response.

1. Implement a Code of Conduct: A good practice for multinational employers is to implement a well-thought-out internal code of conduct or code of business ethics for all affiliate employees worldwide. The code should forbid all acts that the organization has a compelling business reason to prohibit—insider trading, environmental crimes, conflicts of interests, bribery/payments violations, intellectual property infractions, audit/accounting impropriety, discrimination/harassment. Pay particular attention to topics that tend not to be addressed adequately under employment laws, such as social media. Having drafted, communicated and imposed a tough internal code of conduct becomes essential when an allegation of wrongdoing later surfaces and the organization needs to point to a clear rule that prohibited the alleged misdeed. Without a code of conduct, a target may be able to argue he did nothing wrong, or might even claim he had tried to help the organization—for example, by bribing an obstreperous official, by colluding with competitors to raise prices, or by saving money when disposing hazardous waste. Be sure both the code of conduct content and the code launch (rollout) comply with local employment law in each affected jurisdiction.

2. Launch a Whistleblower Hotline: In the United States, communicating a whistleblower hotline to the workplace is a clear best practice to elicit allegations, complaints and denunciations that an employer can then investigate and remedy. By law, publicly traded American companies and "foreign private issuers" must make report "procedures" available for the "confidential, anonymous submission by employees" of their "complaints and concerns regarding questionable accounting or auditing matters." (Sarbanes-Oxley Act of 2002, Pub.L. No. 107-204, at § 301 (1)) Further, America's Dodd-Frank whistleblower bounty program motivates government employers to launch robust international hotlines to lure in whistleblower denunciations that might otherwise go straight to U.S. government enforcers. Liberia and perhaps other jurisdictions have mandated whistleblower hotlines even among non-publicly traded organizations.

But be careful: Overseas, especially in Europe, surprisingly complex regulations closely regulate whistleblower hotlines—Europeans actively invoke data protection laws to rein in American-style anonymous hotlines. Germany, the Netherlands and other EU member states require consulting with employees before launching a hotline. Belgium, France, Spain and other EU states require an employer to make government filings that disclose hotlines, and in some cases a government agency must affirmatively approve a hotline. France, Germany and others restrict hotlines to staff tips about only a limited pool of infractions. Spain and Portugal actually prohibit employers from accepting anonymous whistleblower calls. France seems to prohibit employers from telling their workforces that hotlines accept anonymous calls (The CNIL, France's data protection authority, has flip-flopped on this point). Beyond Europe, in Hong Kong and elsewhere employees may need to consent to a whistleblower hotline. (See Donald C. Dowling, Jr., "How to Launch and Operate a Legally-Compliant International Workplace Report Channel," 45 ABA *The International Lawyer* 903 (2011))

3. Build Channels for Cross-Border Data Exports: An American multinational conducting a cross-border investigation inevitably sends ("exports") back to U.S. headquarters personal information naming or identifying overseas employee

whistleblowers, targets and witnesses. Data privacy laws in *omnibus data protection law jurisdictions*—jurisdictions that regulate all personally identifiable data including Argentina, Canada, Costa Rica, the European Economic Area, Hong Kong, Israel, Japan, Korea, Mexico, the Philippines, South Africa, Switzerland, Uruguay and a growing number of others—expressly prohibit exporting employee data without first building *data export channels*. In Europe these channels are currently "model contractual clauses," "safe harbor," "binding corporate rules" and (in some contexts only) employee consents. (Europe's data protection law regime will get even tougher under an incoming EU data protection "regulation" set to replace the 1995 EU data "directive.") Local data protection laws in Belgium, the Netherlands and elsewhere expressly limit cross-border transmissions of *workplace accusations*, and the EU Article 29 Working Party (the EU's advisory data protection agency) has considered EU-wide restrictions specifically on exporting investigatory data.

Well before launching an overseas investigation in any omnibus data protection jurisdiction, first build channels that will facilitate the export of internal *investigatory* data—or at least verify that the organization's existing data flow channels expressly accommodate the export of investigatory data. Building and expanding cross-border data flow channels can be slow and expensive, and waiting until some specific allegation or suspicion triggers an actual investigation may be too late. Start early.

4. Grant Necessary Data Subject Access: American investigators actively safeguard the confidentiality of their investigation files to protect the integrity of investigations, witnesses and whistleblowers. Counterintuitively, data protection laws in omnibus data law jurisdictions expressly require "data controllers" including employers to disclose personal data including whistleblower denunciations, internal investigation notes, investigation reports and files to the very targets and witnesses identified in the files if they so request. In these jurisdictions, targets and witnesses in internal investigations are "data subjects" who enjoy broad rights to be told that files naming them exist in the first place, and with broad rights to access those files and then ultimately with broad rights to request deletion or "rectification" of investigatory files that name or identify them. (The employer should redact others' names when showing each witness the file.)

In jurisdictions like Hungary, employee rights in this regard are particularly strong. One EU body actually has decreed that employers must tell investigation targets that they are being investigated and that an investigation file exists as soon as there is no substantial risk that notice to the target "would jeopardize" the investigation. (Opinion 1/2006, Article 29 Working Party, 00195/06WP 117 (Feb. 1, 2006)) This said, though, not all data protection laws are so strict in the investigatory context. The British Columbia (Canada) Personal Information Protection Act helpfully offers an *investigatory exception* that relaxes certain obligations to collect employee consents to processing data during internal investigations.

Of course, having to show targets and witnesses investigation files while an investigation is in full swing confounds American investigators. Some American investigators have actually ignored foreign data-access laws in the name of upholding the integrity and confidentiality of their investigations. But of course, any internal investigation that violates local laws is itself illegal activity that some whistleblower could denounce, triggering enforcement proceedings—a scenario every investigator needs to avoid. So in omnibus data protection law countries, always balance investigatory confidentiality against targets' and witnesses' broad legal rights to access data about themselves. Strike this balance *before* a real-world investigation target comes forward and demands access to investigation files during the heat of a pending, high-stakes investigation. As part of an organization's internal investigation framework, articulate a legitimate business case for deferring employee access until the investigation reaches a stable point, and then grant access requests only later, after access becomes legally unavoidable—and after redacting whatever names and information possible. Meanwhile, draft investigation notes and documents cognizant of the fact that the target and witnesses might later access the file.

5. Disclose Investigation Procedures: Europe and other omnibus data protection law jurisdictions might consider an employer's in-house internal investigation framework or protocol a system for processing personal data subject to data laws even before an actual investigation launches and implicates specific personal data about individual employees. Many European jurisdictions affirmatively require that employers disclose, both to the local "Data Protection Authority" and to employee "data subjects," all "personal data processing systems" including any investigatory framework. In addition, labor laws in Europe and possibly elsewhere can require disclosing ("informing") these in-house investigatory frameworks to employee representatives or union committees, like "works councils" and "health and safety committees." Labor laws may require bargaining or "consulting" over investigatory frameworks.

To Americans, all this disclosure and consultation over a simple internal investigation protocol can seem intrusive. Some American lawyers recommend against memorializing investigatory protocols in the domestic American context. But overseas, a multinational that "bites the bullet" and discloses to staff representatives at least a broad outline investigatory framework complies with local data protection laws and frees itself to conduct broader internal investigations later.

B. Responding Initially to a Suspicion or Allegation Arising Abroad

International internal investigation protocol/framework in hand, a multinational is ready to investigate a specific suspicion or whistleblower allegation arising abroad and implicating overseas evidence or witnesses. When a suspicion arises or an allegation comes in, first decide whether it is investigation-worthy—too many multinationals claim to investigate "all" allegations when actually, many accusations prove unworthy of investigating. Some are too vague, some are obviously groundless, some, even if true, amount merely to questionable judgment or rude behavior—and some are mischaracterized human resources gripes best referred to the HR team. Also, be sure the investigation is not just a subterfuge to exonerate the target; that is, verify that upper management will support the investigation, whatever its result. (Avoid the scenario of an investigation report that strongly points to firing a target whom the ultimate decision maker insists on protecting.) As to an investigation-worthy suspicion or allegation, tailor the investigation to the specific allegation and to local laws. Begin with a strategic initial response.

6. Appoint a Qualified Investigator or Investigation Team: Employers often do streamlined investigations into low-stakes allegations with just a single investigator (supervisor, outside expert or lawyer) checking some records and asking some questions. At the other end of the spectrum, a high-stakes, complex internal investigation can be a costly months- or years-long project that mobilizes a team of internal executives, forensic experts, human resources leaders and in-house counsel as well as company directors, outside lawyers, accountants, consultants, private investigators and translators. (*See* Laura Brevetti, "Self Detection: So Key, So Difficult," *New York Law Journal*, July 13, 2009, at S2).

Depending on the stakes and the complexity of a given cross-border investigation, either appoint a single investigator or assemble an investigatory team. Select an investigator or team leader competent in investigatory technique, familiar with applicable law, and experienced with how investigations in the jurisdictions at issue differ from domestic American investigations. Avoid the common mistake of appointing an all-star team of Americans expert in U.S. law, U.S. investigatory best practices, and U.S. criminal prosecutions but with little experience abroad and no understanding of host country law. American investigators tend to focus so intently on the American issues in play that they can get blinded to the compliance challenges under host country employment, data and investigatory procedure laws.

Often a U.S.-led investigation will purposely exclude target-country locals from the investigation team because headquarters might consider the locals inexperienced in internal investigations and susceptible to bias, prone to confidentiality leaks, or too vulnerable to the influence of the local target himself. Where these are legitimate concerns, consider including on

the investigation team at least one local *outsider* (consultant or outside lawyer) familiar with the local players, culture, language and law.

Verify that no one on the investigation team has a conflict of interests or might be a witness. Include on the investigation team someone expert in the subject of the allegation. Consider language fluency. Consider including an investigation team member from the internal audit function and an in-house or outside lawyer who can invoke attorney-client privilege (below ¶ 12). As to outside lawyers, consider tapping investigatory counsel who is *not* the organization's regular advisory counsel and so is less likely to trigger a lawyer-as-witness conflict or to be aligned with interested local managers. Also, think of who beyond the investigation team might need to play a role in the matter—for example, whoever will be involved in imposing discipline or handling grievance procedures (below ¶ 26).

7. Impose Immediate Discipline if Necessary or Impose Interim Discipline: Before taking any other step in an overseas investigation, first check whether local law imposes a *discipline or reporting deadline*. Jurisdictions like Austria impose tight deadlines of only hours or days during which an employer can legally invoke evidence of misbehavior as good-cause support for a firing. France gives employers one calendar month (running from the date the employer gets "informed" of a wrongful act) to impose discipline for cause. (French Labor Code art. L.124-10 *as interpreted by* French Ct.App. dec. no. 38634 of Apr. 3, 2014) In Belgium an employee dismissal for good cause "must occur within three working days from the moment the facts are known to the employer, and then the facts must be notified to the dismissed [employee] by registered mail within three working days from the date of dismissal." (Carl Bevernage, "Belgium" chap. 3 in *International Labor & Employment Laws* vol. IA (ABA/BNA 2014), at pg. 3-38) In Iraq, an employer firing an employee for cause must notify the Iraqi Labour office within 24 hours of the time of the *incident*—not 24 hours after the end of an internal investigation.

In these jurisdictions the "clock" might start as soon as an employer gets solid credible evidence—not after the boss formally wraps up a full-blown American-style internal investigation. In other words, while American employers would argue the discipline "clock" should not start till the investigation ends, that argument might in some situations lose.

Even where local law does not require imposing fast discipline, at the outset of an internal investigation take any necessary interim personnel measures like separating an accused harasser from the alleged victim, or imposing a paid or unpaid suspension until the end of the investigation. But remember that suspended employees become much less cooperative witnesses and may claim the employer constructively dismissed them. For example, the Supreme Court of Canada recently awarded CAN$485,100 in constructive dismissal damages to an executive put on an "indefinite suspension." (*Potter v. New Brunswick Legal Aid*, 2015 SCC 10 (CanL II) (Mar. 6, 2015))

8. Define Investigation Scope and Draft an Investigation Plan: An investigation without a well-defined scope takes unpredictable turns. Remember the outraged criticisms of Ken Starr when his Whitewater investigation abruptly shifted into an investigation of Monica Lewinsky. (*Cf*. Ken Gormley, *The Death of American Virtue: Clinton vs. Starr* (2010) at pgs. 324-62) Delineate the scope of an internal investigation at its outset. Define its goals, set its boundaries—and establish its endpoint. If corporate bylaws require a board of directors resolution to launch an investigation, that resolution should clearly define the investigatory parameters.

In defining the scope of an overseas investigation, factor in the nature of the allegation and the logistical, linguistic and geographic barriers. In some European states, where a whistleblower allegation is anonymous, the fact of anonymity itself restricts the scope of an internal investigation—data protection law in some European jurisdictions deems an anonymous tip to be inherently less credible and less "probable cause" supporting a broad internal investigation leading to discipline.

A good practice is to draft an outline or plan setting out what the investigatory team will and will not do

consistent with the investigation's scope. According to an Australian firm advising on internal investigations:

> "An investigation plan should be drawn up. Key witnesses should be identified, and persons potentially affected by the investigation should be listed. Practical details, such as location and order of witnesses, should be set out. An outline of the questions to be asked should be drawn up. The objective of the investigation should be noted." (Harmer's Work Insights (Australia), Winter 2012, at p. 11)

Any international investigative plan in omnibus data protection law countries needs to account for data subject *access rights in the plan itself* (above ¶ 4). Only if the investigatory plan can somehow avoid identifying the whistleblower, the target and the witnesses, might the plan be exempt from disclosure obligations to data subjects.

9. Comply With Investigatory Procedure Laws: Under American law, a non-government employer's internal investigation is essentially a business matter, not an issue of criminal procedure, because there is no "state action." Other than *Upjohn* and *Weingarten* issues (below ¶¶ 21,23), American internal investigations are largely unregulated. But in some jurisdictions in Eastern Europe and beyond, local criminal procedure laws can restrict and even prohibit a non-government employer or other private party from conducting an investigation. (The policy is that private parties cannot intrude on the exclusive investigatory police power of law enforcement.) In some countries, bar association rules limit or prohibit lawyers (even American lawyers not on the local bar) from conducting internal investigations—particularly if the investigator needs someone to administer an oath, such as for an affidavit or deposition.

Before embarking on any cross-border or foreign local internal investigation, do your research to discover whether any procedural rules restrict private party and lawyer-led investigations. Adapt the investigation to conform. Sometimes it might be a big step just to characterize the internal investigation as mere "analysis," "checking," "verifying" or "asking questions" (below ¶19). And in some contexts it might be possible to conduct the investigation *outside the territorial reach* of local restrictions against private investigations.

Separately, comply with any local laws that require disclosing evidence of a crime to law enforcement (below ¶ 28). And comply with local laws that restrict steps in an internal investigation, like laws regulating how to conduct searches of employee emails/computers/Internet records, searches of lockers and desks, criminal background checking, video surveillance and intercepting phone calls (below ¶17).

10. Research Substantive Law: The purpose of an internal investigation is to uncover evidence of (or exonerate someone suspected of) wrongdoing or illegality. Always ask: Is the alleged behavior wrong or illegal? Violating an organization's internal policies is wrong; violating *applicable* law is illegal. So check both internal policies and applicable law. Internal polices should be clear (above ¶1). But what is applicable law? In overseas investigations, U.S. investigators are susceptible to being lulled by the force of U.S. laws with extraterritorial effect—U.S. trade sanctions laws; U.S. antitrust, securities and discrimination laws; the Foreign Corrupt Practices Act; the Alien Tort Claims Act. Yes, these U.S. laws are "applicable law" abroad because they reach extraterritorially, and yes, these laws are vital. But American investigators sometimes overlook local substantive laws. For example, a U.S. organization's international bribery investigation should, of course, investigate possible breach of the U.S. FCPA and maybe the UK Bribery Act 2010. But investigators should also remember to check for a breach of host country domestic bribery laws. In one situation, an "American businessman" found "guilty of taking nearly US$5.5 million in bribes as head of [a] Dubai-based company" was sentenced to 15 years in a UAE prison even as the U.S. government actually sought to *defend* him. ("U.S. Businessman Gets 15 Years in Dubai Fraud Cases," *Miami Herald*, Mar. 25, 2013).

11. Safeguard but Do Not Guarantee Confidentiality: To guard against data privacy and defamation claims and to avoid human resources and public relations problems arising out of an internal investigation, strictly confine investigation-uncovered

information to company personnel with an actual need to know—the investigation team, retained experts, auditors, counsel, upper management, maybe the board of directors. Resist the temptation to inform too wide a circle as the investigation proceeds. (Whom to brief about the results of an investigation *at the end* is a separate issue, discussed below ¶ 25.) And transmit investigation data back to U.S. headquarters consistent with local legal restrictions on data exports (above ¶ 3).

Unless a self-identified whistleblower expressly consents otherwise, overseas data protection laws may in theory mandate preserving whistleblower confidentiality. But in practice, maintaining whistleblower (and witness) confidentiality can be tough to do where circumstances point to a source and where the whistleblower becomes a complaining witness. Disclosure of a complaining witness's identity is virtually inevitable with a harassment complaint. The best practice is *never to guarantee* whistleblowers or witnesses absolute confidentiality.

12. Secure Legal Advice and Attorney/Client Privilege: Decide who will advise the investigation team on applicable law in relevant jurisdictions. Account for lawyer-as-witness and legal privilege issues, including any foreign law analogue to the U.S. domestic investigatory-context privilege. (*See* E. Herrington & T. McCann, "Privilege Pitfalls: Companies Must Be Careful to Preserve Right During Internal Probes," *Corporate Counsel*, July 2014 at pg. 35; L. Krigten,"Waiver of Attorney-Client Privilege to Protect the Company" *Nat'l Law Journal*, Nov. 22, 2012 at 16; J. Nathanson, "Walking the Privilege Line," *New York Law Journal*, July 13, 2009, at S8.) A Canadian law firm recommends, as to Canadian internal investigations: "Give some thought…at the very beginning of the process, as to whether you wish the investigation process, report and surrounding communications to be privileged. It is much easier to attempt to set this up at the beginning of the [investigation] than mid-way through." (Rubin Thomlinson LLP (Toronto), *Workplace Investigation Alert #14* (Aug. 2012)) While the attorney-client privilege can be vital in an internal investigation, *discovery* is far less robust abroad, and so attacks on the attorney-client privilege are much less frequent overseas—a fact that American litigators often forget. But foreign government agents occasionally seek documents from private parties, and a foreign privilege issue can arise in a U.S. proceeding.

Assess whether lawyers on the investigation team can invoke the attorney/client privilege under applicable local law. Depending on the jurisdiction, the local privilege may reach locally licensed outside law firm counsel and maybe locally licensed in-house counsel— although jurisdictions like China may not recognize any attorney-client privilege. Always check whether a jurisdiction extends its attorney-client privilege to foreign, such as U.S., lawyers not on the local bar. (Never assume a U.S.-licensed lawyer falls under a foreign-law attorney-client privilege.)

Privilege issues are much less settled in jurisdictions outside the common-law world. In some jurisdictions the privilege actually belongs to the *lawyer*, not the client. Some European Union member states recognize a rudimentary in-house counsel privilege, but there is no European-wide doctrine that confers a privilege on in-house counsel. (*Akzo-Nobel*, ECJ case c-550/07P (9/14/10)) Hungary, for example, does not offer any reliable in-house lawyer privilege, and in France lawyers who go in-house must resign from the bar and surrender any claim to privilege. Secondary sources are inconsistent addressing privilege abroad.

13. Account for U.S. Government Enforcement Issues: American multinationals increasingly launch cross-border internal corporate investigations responding to inquiries or enforcement actions from American agencies like the Department of Justice [DOJ], the Securities Exchange Commission [SEC] and (potentially) the Equal Employment Opportunity Commission. Internal investigations responding to U.S. government inquiries and proceedings raise unique issues of U.S. government-context attorney/client privilege waiver and advancing defense fees, and the issue of a "corporation's timely and voluntary disclosure of wrongdoing and its willingness to cooperate in the investigation of its agents, including, if necessary, the waiver of corporate attorney-client and work product protections." The U.S. government has taken formal but changing positions here. This issue is beyond the scope of this article, but should be carefully considered.

How these U.S.-law government privilege, defense fee and voluntary disclosure issues play out in scenarios arising *outside the United States* gets even more complex. Indeed, the various U.S. government positions and memos here have been criticized because they are said to ignore or downplay the analysis under foreign law. And American prosecutors might fail to understand and appreciate mandates under foreign laws. Where U.S. government privilege, defense fee and voluntary disclosure issues arise overseas, proceed carefully.

14. Safeguard Disclosures to and From Experts: Always have any retained outside experts (including any private investigator, forensic accountant, forensic computer specialist, investigation consultant, e-discovery provider, translator) contractually commit to uphold confidentiality and applicable data protection laws. Safeguard the attorney/client privilege over disclosures to experts (above ¶ 12). In Europe and other omnibus data protection jurisdictions, an expert's report identifying specific individuals may be subject to disclosure to witnesses, and even to investigation targets (above ¶ 4). Proceed carefully.

15. Impose an Enforceable Litigation Hold: Spoliation claims (destruction of documents relevant to litigation) are increasingly common in domestic American lawsuits, even as spoliation remains a rare cause of action abroad. A best practice is to require that employees in affected countries preserve data possibly relevant to a cross-border investigation at least until the investigation and any litigation wind down and maybe even until all statutes of limitations run. During internal investigations, multinationals often order staff, across borders, to suspend routine data destruction practices like automatic email deletion and document-destruction policies and to disable computer programs that swab or erase electronic data. Software exists for implementing and enforcing these internal retention orders—often called "litigation holds" or "DRNs" (document retention notices).

Outside the United States, litigation holds/DRNs can be vital but they are less routine and so are less familiar. Fortunately an overseas litigation hold/DRN raises few legal hurdles. But *better explanations and enforcement* become important in countries where these holds are less familiar.

That said, in Europe and other omnibus data protection jurisdictions, an overbroad litigation hold/DRN kept in place too long butts into the data protection law prohibition against retaining obsolete personal information. In jurisdictions that require purging obsolete personal data, be sure to articulate a defensible business rationale for any long-term litigation hold. Review the need for the hold regularly.

16. Secure Evidence Within Management's Physical Custody: Collect and preserve relevant documents and electronic files that management already has in its possession (before breaking into employee-held files). Data laws in omnibus data protection law countries may prohibit management from "processing" for investigatory purposes even information already in company files unless the original reasons for collecting the data had expressly included "investigatory purposes" (which is rarely the case). Therefore, when structuring HR data processing and export systems, be sure specifically to include "processing/storing personal data for internal investigatory purposes" as one of the designated reasons for personal data processing (above ¶5). And because data laws can restrict "exporting" personal data to American headquarters, consider warehousing investigatory information locally in a host country without transmitting it stateside, unless compliant data export channels are in place (above ¶3).

17. Gather Evidence Outside Management's Physical Custody: Perhaps the biggest single hurdle in overseas investigations is how, legally, to gather employee documents and data *not yet in management's* readily *accessible files*—emails on the company server, Internet-use records, Word documents on an employee's hard-drive, papers in an employee's desk, and administering any tests like post-accident drug testing, polygraph or drug residue tests. Seizing an employee's laptop or personal device for a search requires coordinating with the IT group and timing considerations, to minimize the employee's opportunity to destroy evidence.

American law, by international standards, is employer-friendly in letting bosses collect data from staff. The other side of that coin is that American employers get surprised, overseas, at how tough it is to gather data from their own staff during an investigation. Staff in Europe and elsewhere may firmly believe that their personal business records—even though warehoused on company systems formally designated as "company property"—are off-limits to their employer. Foreign local data protection laws can actually support this view, even if the employer had issued a policy purporting to reserve its ownership of, and its right to search, company data systems, and ostensibly defeating employee expectations of privacy in their data.

Employer reservation-of-right-to-search policies are just as vital internationally as they are stateside, but are not as *effective*. When operating outside the United States, American headquarters should not assume that a stated reservation of the right to search overseas employee computers and cubicles will work as it does stateside. Abroad, employer reservations-of-right-to-search may be a mere *first step* in analyzing whether or how the employer can legally access staff emails/Internet records/documents. For example, in Alberta, Canada, an employer usually cannot read employee emails unless the employee has consented in advance to the search. (*Moore's Industrial Svc. Ltd.*, Alberta Office of Info. & Privacy Comm'r order # P2013-07, Nov. 29, 2013, at ¶ 53). And laws in Europe, even in England, make it particularly difficult for any employer ever legally to read an email that an employee had been clever enough to mark "PERSONAL" in the subject line. In a 2013 Chinese case, even though the employer's code of ethics had told employees that emails on company servers were "company property rather than personal communication," the Guangdong Foshan Intermediate People's Court held an employer's review of staff emails during an internal investigation was flatly illegal.

Understanding when and how foreign law lets employers search their own employees' electronic and physical files is a research project unto itself, and so to list all the steps employers must take to search employee emails, computer records and physical spaces outside the United States is a discrete topic under local law in each jursidiction, beyond the scope of our discussion here. Do a country-by-country analysis of all jurisdictions implicated in the investigation in light of the specific facts. In Continental European jurisdictions like Austria, Italy, Germany and Poland, a key issue in this analysis will be whether the employer had previously forbidden local staff from using company-owned computers/systems even for incidental personal use In fact, *telecommunications* laws actually come into play here and regulate whether an employer can get into its own staff's emails in the organization's computer system. In some countries a key issue will be whether employees had granted "unambiguous," situation-specific consents to search, especially in the "bring your own device" [BYOD] context.

Even where an employer has purported to reserve its asserted "right" to access employee emails/Internet use/documents, always get tailored advice under foreign law before actually conducting a search (and certainly before ordering polygraph or drug tests, which are very rare outside North America), or before launching surveillance tools or video monitoring, or before surreptitiously monitoring employees in other ways. It has been said that multinationals should take "caution"; reviewing employee documents in an overseas investigation "should be subject to local legal review." (K. Cooper-Franklin & T. Tyson, "Global Investigations: A Six-Step Process," *HR Magazine*, Nov. 2013 at pg. 47, 48) Local procedural mandates on these topics can be unpredictable. In France, for example, an employer must get a court officer or bailiff and bring him in to oversee its accessing staff files and documents.

C. Interviewing Witnesses Abroad

After securing documents it becomes time to interview witnesses. Work out a strategic order for interviews, such as accuser, then witnesses, then target. Work up strategic outlines for the interviews, such as going from the general to the more specific. In conducting each employee interview, factor in overseas cultural and strategic issues. During interviews, comply with local employment and data protection laws and think ahead

to compliance with laws regulating discipline and dismissals.

18. Verify Sources and Try to Interview the Whistleblower: Where communication channels to an *anonymous* overseas whistleblower remain open, before doing any interviews first try to coax the whistleblower to self-identify and be interviewed. Overseas, when interacting with a whistleblower or complainant who kicked off an internal investigation, check whether the accuser will stand by the accusations. Firm up the source of the allegations and seek corroborating evidence and witnesses.

This step is counterintuitive to American investigators, because various state and federal statutes protect the anonymity of whistleblowers, but it is important, overseas, for whistleblowers to self-identify: As mentioned (above ¶ 8), under law in Europe an investigation into an anonymous whistleblower tip cannot plow as deep as an investigation into a denunciation from a verified source.

19. Neutralize or "Demilitarize" Interrogations: Sometimes an American interrogating a foreign employee conveys an air of professionalism and authority that, overseas, may prove counterproductive and culturally inappropriate. The witness might "clam up." Neutralize the international interrogation process by "demilitarizing" witness interviews, coaxing out better information with a softer touch.

For example, while an internal investigator's background as a former U.S. prosecutor may enhance investigatory credibility stateside, overseas that background might be off-putting—foreign witnesses actually have alleged *harassment* when questioned by an interrogator who introduced himself as an American ex-prosecutor expert in criminal law. American witnesses might respect police authority, but abroad, downplaying any prosecutorial credentials and criminal law expertise on the interviewer's résumé usually opens up a foreign witness and lowers the chances of collateral harassment allegations stemming from the interview itself. In fact, a case could be made that former U.S. prosecutors, supremely qualified to conduct domestic American internal investigatory interviews, actually suffer certain disadvantages when they travel abroad to question witnesses in foreign contexts where U.S. criminal procedure does not apply.

When questioning employees overseas, one strategy is to neutralize the semantics of the interrogation itself. Investigators might refer to their internal investigation and their interrogation as merely "some questions," "talks," "checking" or "verifying." They might refer to an allegation, suspicion, complaint or denunciation as merely an "issue" or "question." Documentary evidence and proof might be mere "papers" or "files." Whistleblowers, informants, sources and witnesses might simply be "employees" or "colleagues" (those not on the payroll are "business partners"). Call the target of an investigation "our colleague." And an investigator zeroing in on a confession might request a mere "affirmation" or "acknowledgement."

When conducting staff interviews, always be sensitive to local conceptions of privacy. Outside the United States, expect employees to believe they have some sort of right to refuse to answer personal questions about their sex lives, hobbies, families, workplace friendships, incomes and their personal notes, documents, emails and social media postings. In overseas investigatory interviews, show sensitivity for this view—even if, to American investigators, it seems misinformed.

20. Instruct Witnesses to Cooperate Only as Permissible: An American investigator ghostwriting an employers' memo announcing an internal investigation might reflexively declare that all employees "must cooperate" with the internal investigation. And American investigators like to begin employee interviews by insisting that each witness "must cooperate." This approach may be appropriate under U.S. employment-at-will, but it can backfire abroad because it is often simply not true: Foreign employees usually do not have to cooperate with an internal investigation. Employees often enjoy a labor-law right to remain silent roughly analogous to the American Fifth Amendment in the police-investigation context.

Never assume an employer will have "good cause" to fire a non-U.S. employee who refuses to cooperate in an internal company investigation. When an overseas

witness folds his arms, shuts his mouth and tells investigators he will not talk, labor law doctrines in many countries support him. Indeed, whistleblowing rules in Europe actually forbid employers from unilaterally imposing mandatory reporting rules (for example, in codes of conduct) that force witnesses to disclose incriminating information about their coworkers (above ¶2). An employer order (as opposed to a request) to "cooperate" with an internal investigation likely triggers the same legal barriers and might be an impermissible mandatory reporting rule.

The point is simply that investigators should speak accurately overseas and think carefully before reflexively commanding employees to "cooperate" in internal investigations or investigatory interviews. The investigator needs to know whether employee witnesses have a right to remain silent.

21. Comply With Collective Consultation and Witness Representation Rules: Labor laws in Finland, France and elsewhere in effect require consulting with local employee representatives (union committees or works councils) before investigators launch a slate of staff interviews. American investigators who burst into an overseas workplace and start questioning staff without first having given local management a chance to confer with local labor representatives about the inverviews can commit an unfair labor practice.

A related issue is foreign local *Weingarten* rights. (*Cf. NLRB v. Weingarten, Inc.*, 420 U.S. 251 (1975)) In jurisdictions including the United States, to interrogate employee witnesses who may be implicated in allegations and subject to discipline without letting them bring representatives can be an unfair labor practice (just as a lawyer interrogating a witness known to be represented by counsel without notifying that lawyer may breach ethics rules). Be sure to respect mandatory interview-context representation rights. In England, an employee has "a statutory right to be accompanied by a companion" at a disciplinary hearing, but not a routine investigatory meeting, after making a "reasonable request." (ACAS *Code of Practice on Disciplinary and Grievance Procedures*, Mar. 2015 at ¶¶13, 15) Employees in Europe occasionally invoke article 6(3)(c) of the European Convention on Human Rights to argue they have a right to bring a *lawyer* to investigatory interviews (although the Convention only extends that right to those "charged with a criminal offence").

22. Notify Targets and Witnesses of Their Rights: American police read criminal suspects their Miranda rights, but in the non-government workplace investigation context an American employee witness has few if any affirmative rights (beyond *Weingarten*, above ¶ 21 and *Upjohn*, below ¶ 23). Not so abroad. Staff in many countries enjoy robust procedural rights in the workplace investigation context. One sweeping right in Europe is the right to be told precisely what your other investigatory rights are. Even in countries outside Europe where local law does not force internal investigators to brief witnesses on their rights, a local best practice may be to begin an investigatory interrogation by advising each witness of his due process protections.

Further, as mentioned (¶ 4), data law in Europe and elsewhere requires telling targets and witnesses about internal investigation notes and files that identify them and then requires offering targets and witnesses limited access to investigatory files and a right to "correct" them *even while the internal investigation is still pending*. This right directly conflicts with the American investigatory best practice of keeping unfolding investigations strictly confidential. So strike a balance to comply with legal mandates. Genuinely "anonymizing" names and identities in investigation files eliminates the data-law disclosure obligation here. But in the context of an active investigation, anonymizing is rarely practical.

23. Give *Upjohn* Warnings, Demand Witness Confidentiality and Conduct Interviews Legally: A lawyer interviewing domestic American employee witnesses in an internal investigation should always give so-called *Upjohn* warnings (*Upjohn v. U.S.*, 449 U.S. 383 (1981)) telling each staff witness that the investigator represents the employer and may be covered by confidentiality obligations and attorney-client privilege, and explaining that the employer might waive its privilege and offer interview information to third parties including law enforcement. (*See* R. Jossen & N. Steiner, "The Upjohn Pitfalls of Internal

Investigations;" *New York Law Journal*, July 13, 2009, at S4) As U.S. domestic law, *Upjohn* is not authoritative abroad, but giving *Upjohn*-style warnings is a clear best practice worldwide.

Beyond *Upjohn*, investigators should always instruct overseas employee witnesses to keep the interrogation and investigation strictly confidential, not discussing it with anyone. Indeed, to let a (foreign) witness talk about a pending internal investigation could actually violate overseas data protection laws. This may sound simple and obvious, but actually American investigators have recently gotten gun-shy about instructing witnesses to preserve confidentiality because as of 2012, demanding employee confidentiality in domestic American investigatory interviews risks violating American labor law as an impermissible restriction on "protected concerted activity." (*See Banner Health System*, 358 NLRB No. 93 (2012), *questioned by Canning v. NLRB*, case no. 12-1115 (D.C. Cir. 2013)) Savvy American investigators, therefore, have actually stopped demanding confidentiality of stateside investigatory witnesses. But we can confine this issue to U.S. soil. The broad American "protected concerted activity" doctrine is all but unknown overseas, even in common-law countries and even in Canada. And so *Banner Health* raises a purely domestic American issue. Multinationals should always impose a confidentiality mandate on overseas witnesses. There is no good reason to extend the *Banner Health* doctrine abroad.

Upjohn warnings and *Banner Health* confidentiality issues aside, be sure to conduct overseas investigatory interviews legally, in compliance with local criminal procedures. For example, be careful asking staff to tell you what they have told local police in criminal-context interviews—some jurisdictions prohibit this line of questioning. As another example, when recording staff interviews, first get recording consents from witnesses that comply with local data protection law, in writing as necessary.

D. Discipline, Remedial Measures and Post-Investigatory Communications in Cross-Border Investigations

After collecting documents and conducting investigatory interviews in an internal investigation, what had been an information-gathering process at last becomes active decision-making. Decide on the investigation findings. Impose discipline and implement remedial measures. Take these steps consistent with applicable employment, data protection and criminal procedure laws. Memorialize, preserve and report on investigation results consistent with applicable data protection laws.

24. Involve the Audit Function and Comply With Accounting Rules: Where an investigation uncovered financial impropriety, money losses or bribery/improper payments, tackle the accounting and financial-statement issues. Involve the audit function. Comply with U.S. Foreign Corrupt Practices Act accounting (payment-disclosure-reporting) rules as well as Sarbanes-Oxley accounting mandates and applicable Generally Accepted Accounting Principles. Financial losses at an overseas affiliate reach the "bottom line" of a U.S. parent, so at a publicly traded multinational an overseas investigation might implicate U.S. securities mandates and auditing/accounting disclosures. Manage strategy with inside and outside auditors. Implement auditor/accountant recommendations.

25. Report to Upper Management: Consider the pros and cons of delivering an oral versus a written report to upper management detailing the investigation findings. Limit the circle of upper management receiving an investigatory report to those with a demonstrable need to know. Keep in mind restrictions on "exporting" investigation data and data subject rights of access to a final written report (above ¶ 3). Data protection laws and privilege rules as well as discoverability in U.S. proceedings may weigh against a written report. Draft any investigation summary report carefully with findings of fact grounded in the evidence. Consider whether the report can remain privileged. Refrain from declaring anyone guilty of a

crime—internal investigators are powerless to declare guilt in any criminal justice system, and some investigators believe the word "guilty" does not belong in a private internal investigator's vocabulary.

26. Impose Post-Investigatory Discipline Consistent With Procedural and Anti-Retaliation Mandates: Where an investigation uncovers solid evidence of wrongdoing (and where the employer did not already take final disciplinary action at the beginning of the investigation, above ¶ 7), impose discipline consistent with investigation findings and consistent with upper management buy-in. If the investigation exposed enough evidence to dismiss the suspect for good cause under local law, then structure the dismissal to be for good cause. But sometimes an investigation uncovers enough evidence of wrongdoing to convince an employer to dismiss the target but not enough to support a good-cause dismissal under applicable employment law. In those situations the employer (where legal) might decide to dismiss the target without cause, paying notice and severance pay.

In dismissing someone (whether or not for good cause), follow local-law dismissal procedures. Chad, France, the United Kingdom and many other countries impose detailed procedures on employers firing even obviously culpable staff; these procedures can involve complex notice procedures and grievance filing and appeal rights. (E.g., U.K. ACAS Code of Practice on Disciplinary and Grievance Procedures, Mar. 2015 at ¶¶18-47) In omnibus data protection jurisdictions, having followed data law during an internal investigation becomes vital at the discipline stage because employees in these jurisdictions increasingly allege data law breaches when they get disciplined.

When disciplining a witness, whistleblower or target who could plausibly claim to have lodged a workplace complaint, consider local foreign anti-retaliation laws like the laws in Europe that prohibit "victimizing" whistleblowers. American-law anti-retaliation prohibitions are particularly strict, but most court decisions construing the extraterritorial reach of U.S. retaliation law tend to confine these protections to U.S. residents.

27. Ensure Internal and External Communications Comply: With confidentiality so paramount in internal investigations, a multinational might prefer to keep its investigation results under wraps. But in the real world, especially in high-profile cases, internal and even external communications about an investigation can be necessary. Employees may demand to know what happened, and word of some internal allegations might inevitably make social media or news sites. In at least one high-profile American internal investigation, for example, television stations actually interrupted their regular programming to report on the release of an employer's internal investigation report.

As to post-investigation reporting, a good first step is to close the loop with the original whistleblower (where that channel remains open). Tell the whistleblower what the investigators found out and what the employer will do about it.

In internal and external reporting about an investigation, be alert to defamation and tortious invasion of privacy claims. Ensure that mentions of the investigation and the fate of the target are defensible. Again, avoid the word "guilty." Heed applicable data-law restrictions against disclosing and exporting personal information.

28. Disclose to Authorities Appropriately: Consider turning over to local police or enforcement authorities investigation-uncovered evidence of criminal acts, especially where applicable law imposes a self-reporting obligation. Local law in some jurisdictions actively requires denunciations to local police. Slovakia, for example, requires that parties including employers with knowledge of a criminal act notify authorities. (Slovak Crim. Code no. 300/2006) New South Wales, Australia requires that parties including employers with evidence about a "serious indictable offence" report to local police. In England, for-cause dismissals in the financial services sector may have to be reported to authorities on "Form C" under the "FCA" and "RPA" handbooks. Heed these reporting mandates.

However, where these mandates do not apply and absent a court order, data protection law in some jurisdictions actually restricts an employer's freedom to volunteer, even to government law enforcers, information learned in an internal investigation. Reporting to police could also raise an employment law challenge—fired staff in some jurisdictions (France, for

example) might actually argue that a police denunciation amounts to additional, illegal employer discipline: Under local employment law, a dismissal may be legal but a dismissal plus a denunciation to police may be excessive discipline.

29. Implement Appropriate Remedial Measures: Implement remedial measures—steps to prevent the problem from recurring, like new work rules and new tools for oversight, security, monitoring and surveillance. But check that these new measures comply with substantive laws like data protection rules restricting employee monitoring. Collective labor representation laws and vested/acquired rights concepts restrict an employer that wants to tighten terms and conditions of employment by imposing unpopular new security measures without first consulting with staff representatives. Overseas, an employer cannot always unilaterally start surveillance (video or computer monitoring, for example) without employee consent. For that matter, this is also the rule in the U.S. union context. (Cf. Brewers v. Anheuser-Busch, 414 F.3d 36 (D.C. Cir. 2005))

30. Preserve Investigation Data Appropriately: Preserve the investigation file (notes, interview transcripts, expert reports and summary report) consistent with applicable law and investigatory best practices. "The details of every investigation should be memorialized in writing, regardless of the findings, including a description of the allegation, the steps taken to investigate it, factual findings and legal conclusions, and any resultant disciplinary or remedial actions"—and then, of course, the employer retains that "writing" in case it may be needed later. (S. Folsom, V. McKenney & P.F, Speice, "Preparing for a Foreign Corrupt Practices Act Investigation," ABA International Law News, Winter 2013 at p. 6) Even where an investigation finds no probable cause, investigation records are invaluable if a similar allegation later arises involving the same suspects.

But the American practice of retaining investigation documents can be flatly illegal abroad. In some jurisdictions, simply preserving an investigatory file conflicts with the data-law duty to purge obsolete personal information when there is no compelling business case to retain it. Indeed, recent caselaw in Europe actually invalidates local European laws that had been implemented to try to mandate retaining certain documents for short periods to make them available for police investigations—European courts strike down these laws because they violate the data-law duty to purge personal data promptly. (Digital Rights Ireland v. Seitlinger, EU Ct. Justice, decision of Apr. 8, 2014; Privacy First Foundation v. Netherlands, Netherlands Dist. Ct., The Hague, Mar. 11, 2015; but cf. Australia's Telecommunications Interception and Access Amendment Data Retention Bill of 2014, passed in March 2015, requiring retaining "metadata" for law enforcement evidence purposes)

Of course, there may be many business reasons for retaining investigation records indefinitely. The challenge is that data protection authorities (at least in parts of Europe) could reject that argument as spurious. This can mean destroying or completely anonymizing an investigation file (including even an unanonymized investigation summary report) surprisingly soon after an investigation ends—within two months, under one influential EU recommendation, at least where the investigation did not lead to discipline (Opinion 1/2006, supra ¶ 4) That said, sometimes an employer might be able to justify retaining an investigation file at least until any relevant statute of limitations runs.

* * *

American best practices for investigating a suspicion or allegation of employee wrongdoing are well-developed. U.S. multinationals believe in the value of these evolved American investigatory practices, and so American organizations looking into an allegation overseas like to export these practices—especially when a domestic American complaint alleging a violation of American law implicates evidence or witnesses abroad. But exporting U.S. internal investigatory practices requires advance planning, flexibility, adaptation and compromise. Always adapt U.S. investigatory strategies to the very different realities and seemingly quirky legal mandates of the overseas workplace.

K&L GATES

Anchorage Austin Beijing Berlin Boston Brisbane Brussels Charleston Charlotte Chicago Dallas Doha Dubai Fort Worth Frankfurt Harrisburg Hong Kong Houston London Los Angeles Melbourne Miami Milan Moscow Newark New York Orange County Palo Alto Paris Perth Pittsburgh Portland Raleigh Research Triangle Park San Francisco São Paulo Seattle Seoul Shanghai Singapore Spokane Sydney Taipei Tokyo Warsaw Washington, D.C. Wilmington

K&L Gates comprises more than 2,000 lawyers globally who practice in fully integrated offices located on five continents. The firm represents leading multinational corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit klgates.com.