## TABLE OF CONTENTS

I. Introduction ................................................................................................................................. 1

II. Overview of EU Data Privacy Laws .......................................................................................... 3
   A. EU Directive 95/46/EC ............................................................................................................... 3
   B. Key Concepts ........................................................................................................................... 5
   C. Data Privacy & Investigations - General Observations .......................................................... 8

III. Investigations & Data Privacy - Implementing Protective Measures and Evidence Gathering ........................................................................................................... 11
   A. Pro-Active Employee Monitoring ............................................................................................ 12
      1. Maintaining Transparency and Ensuring Openness .............................................................. 13
      2. Avoiding Disproportionate Data Collection ........................................................................ 15
      3. Ensuring Appropriate Retention and Security ..................................................................... 17
      4. Transfers of Information to Third Countries ........................................................................ 19
      5. Additional Considerations ..................................................................................................... 20
   B. Inviting the Submission of Probative Information .................................................................... 21
      1. Whistle-Blowing Hotlines: Background ............................................................................... 21
      2. Current Status of Whistle-Blower Devices .......................................................................... 23
   C. Due Diligence Involving Third Parties .................................................................................... 27
      1. Maintaining Transparency of Information Collection ........................................................... 28
      2. Avoiding Disproportionate Collection .................................................................................. 30
      3. Transfers of Information to Third Countries ........................................................................ 30

IV. Investigations & Data Privacy - Conducting Wide-Ranging Investigations into Possible Wrongdoing .................................................................................................................. 32
   1. Maintaining Transparency and Competing Considerations .................................................... 33
   2. Ensuring a Legitimate Basis Exists .......................................................................................... 36
   3. Avoiding Disproportionate Data Collection ............................................................................ 39
   4. Ensuring the Security of Gathered Data .................................................................................. 40
5. Handling Requests to Access Data ................................................................. 42

6. Considerations Related to Transferred Data ............................................. 43

V. Investigations & Data Privacy - Targeting Specific Individuals Based on Credible Information......................................................................................... 45
   1. Withholding Notice to Relevant Parties .................................................. 46
   2. Ensuring a Legitimate Basis Exists.......................................................... 47
   3. Avoiding a Disproportionate Investigation............................................ 50
   4. Responding to Access Requests.............................................................. 52
   5. Transfers of Information to Third Countries ........................................ 52

VI. Investigations & Data Privacy - Issues Upon Completion .......................... 54
   1. Retaining Investigative Data................................................................. 55
   2. Complying with the Finality Principle.................................................. 56
   3. Responding to Access Requests.............................................................. 56
I. INTRODUCTION

Enron, Parmalat, Network Associates, DaimlerChrysler, Hollinger International, Wal-Mart -- every day, the list of organizations committed or compelled to undergo internal investigations to address allegations of potential or suspected wrongdoing gets longer. They may be investigating whether they have violated applicable laws, for instance laws governing accounting practices, anti-bribery rules, or money laundering regulations, or whether significant internal corporate policies, such as policies prohibiting harassment in the workplace, have been infringed. These investigations may be internally devised and driven, with the organization hoping to identify and address any problems well before the authorities step in to do the job. Or, worse, the investigations may be demanded by law enforcement or regulatory bodies enjoying broader regulatory mandates and increased resources, who may have brought their suspicions to the management’s attention after keeping a close eye on the company’s conduct. In some cases, the investigation may be tied to ongoing or anticipated litigation, possibly litigation conducted overseas.

In these circumstances, the urge to go to any and all lengths to the find the culprits can be overwhelming. Senior management, shareholders and authorities want the responsible persons found and found quickly. No expense is spared and plenty of midnight oil is burned as employees are interviewed, computer hard-drives scanned, e-mails and other communications reviewed. Teams of external lawyers may be engaged, assisted by legions of consultants well-armed with laptops and notepads. Documents, reports, e-mails and anything else of potential relevance to the investigation may be circulated far and wide by post, facsimile and the Internet. Everyone understands what is at stake: the company’s reputation, criminal or civil liability, perhaps even imprisonment for the guilty.

No wonder then that many organizations, when faced with the realities, the pressures and the implications of such investigations, frequently put all other considerations to the side.
Data privacy rights are a secondary concern, assuming they are a concern at all. Quite frequently, the issue is remembered too late -- data privacy rights have been flouted or simply ignored and personal data processed unfairly, insecurely, and in blatant violation of the law. And so, in trying to clean up one problem, the organization unwittingly creates for itself another, by engaging in flagrant breaches of data privacy laws whose consequences will come back to haunt it.

This paper focuses upon the intersection of European data privacy laws and corporate investigations. It describes the data privacy issues that are likely to arise in the context of an investigation undertaken by an organization and offers some suggestions for how to best handle those issues to avoid falling afoul of the law. In this author’s opinion, the precise nature of the interplay between data privacy laws and investigations tends to vary depending upon the stage at which an investigation has reached. For instance, an organization conducting preventative or pro-active monitoring of employees or performing due diligence about business partners, before any wrongdoing is known or believed to have taken place, will be much differently placed -- in data privacy terms -- from an organization that reasonably suspects that a person or persons have engaged in criminal behavior.

For this reason, this paper is divided into four sections, reflecting four different “phases” of an investigation; although these “phases” remain artificial constructs, they are helpful when examining the data privacy implications of a corporate investigation. First, we examine the pre-investigation stage, focusing on the issues arising from an organization’s deployment of prophylactic measures, particularly employee monitoring, whistleblower hotlines and information-gathering tools on business partners, before any actual wrongdoing is known or believed to have occurred. These efforts are designed to ensure the rapid detection of employee activities or business dealings that would trigger a more detailed investigation. We focus in particular on the use of whistleblower hotlines, which have
attracted a great deal of attention from European privacy regulators, particularly those in France.

Second, we turn to the next investigative stage - the point at which an organization has reasonable grounds for suspecting that a person or persons within the organization may have violated applicable laws or regulations or breached critical internal corporate policies. This stage of an investigation generally is accompanied by wide-ranging efforts to gather information that could both determine whether any impropriety has occurred and identify the responsible persons within the organization. It often requires a company to interview a large number of staff and amass a mountain of potentially relevant (and much irrelevant) data.

Third, we discuss the issues surrounding investigations that have proceeded to a more mature stage – this is the point at which an organization actually has a reasonable, targeted suspicion that a particular person or persons, which could be employees or external third parties, may have committed some crime or become involved in improper activities that are associated with the organization. The outcome of this stage will either be the apprehension and punishment or exoneration of suspected wrongdoers.

Finally, we look at the post-investigation data privacy issues that an organization may encounter and should consider. These include, for instance, an organization’s retention of documents or materials generated from an investigation and so forth. Although we assume some basic familiarity with European data privacy laws, we start with a brief overview of the European Union’s (EU) data privacy regime to situate the ensuing discussion.

II. **OVERVIEW OF EU DATA PRIVACY LAWS**

A. **EU Directive 95/46/EC**

The EU’s data protection regime, although one of the earliest to emerge, remains of relatively recent vintage. In the 1970s and early 1980s, a number of European countries enacted legislation specifically intended to enhance the level of privacy protections enjoyed
by individuals in those countries, including novel protections for information relating to or about them. These national legislative developments paralleled, and were often influenced by, broader regional and international efforts to safeguard personal data. Both the OECD’s 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the Council of Europe’s 1981 Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data,\(^1\) served as the bases for further legislative developments. But despite this emerging framework of supranational data protection principles and laws, Europe’s national data protection regimes continued to diverge in important respects, thus impeding transborder flows of personal information. In the most famous example, the French national data protection authority blocked transfers by Fiat France of employee data to Fiat’s headquarters in Italy, claiming that the data would not be properly protected without French regulatory oversight.

In response to the obstacles posed by Europe’s divergent approaches to data protection, the EU sought to facilitate free movement of personal data among EU Member States by harmonizing data protection legislation. In 1995, the European Parliament and the Council of Ministers adopted Directive 95/46/EC to establish a set of uniform provisions governing the processing of personal data in the EU (the “Data Protection Directive”).\(^2\) The Directive required all EU Member States to enact implementing legislation by October 25, 1998. Although some, in fact many, Member States failed to meet the 1998 target date -- France, for instance, only enacted implementing legislation as late as 2004 -- all 27 EU Member States have managed to implement the Directive, including the 12 Central and Eastern European countries that recently joined the EU. Although the Data Protection

---

\(^1\) Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (Jan. 28, 1981).

Directive is the key piece of privacy legislation in the EU, there are other laws about which organizations should be aware. In 2002, in particular, the European Parliament and Council enacted European Directive 2002/58/EC, which lays down specific data protection rules for the electronic communications sector.3

B. Key Concepts

The Data Protection Directive’s overarching purpose is to protect the right of natural persons to privacy with respect to the processing of their personal data.4 The Directive covers all “personal data,” defined as information relating to an identified or identifiable natural person, or “data subject.”5 It imposes obligations directly upon persons or organizations that determine the purposes and means of processing personal data, so-called “data controllers.” In the investigative context, a company undertaking an investigation should be positioned as a controller with respect to any personal data that are gathered by the company or its agents (e.g., consultants or legal counsel).6 “Processing,” in turn, encompasses everything done with personal data, from collection to destruction. The Directive’s expansive terms bring almost any operation involving personal data within the scope of the law. It applies to personal data handled by computer or other electronic means, as well as personal data held manually in a filing system (such as card indices, microfiche, or paper files). Personal information that does not reside in an organized system of files (e.g., personal information contained in a stack

5 Id. Art. 2.
6 As discussed below, it could be argued that external legal counsel or outside consultancy firms, to the extent that they are subject to independent professional or legal obligations with respect to their handling of any materials (including personal data) procured during the course of the investigation, are co-controllers of such data. The law, at present, remains unclear, and clarifying regulatory guidance has not been released.
of letters sitting on a desk, scattered throughout an office) may not be covered, although national data protection authorities are likely to construe this exception narrowly.

The Directive has broad scope, and applies to private and public organizations established in the EU that collect or otherwise process personal data and organizations that, although not established in the EU, use equipment located there to process personal data. And, broadly speaking, two distinct obligations arise where the Directive applies to an organization handling personal data as a data controller. In those EU countries where there is a notification procedure (which is the vast majority), the organization typically is required to notify its local privacy regulator. Further, it is required to comply with basic principles of data protection that regulate the manner by which data can be collected, held and processed. Those principles are the following:

- **Fair and Lawful Processing**: Personal data must be processed fairly and lawfully. Typically, this requires that the organization furnish certain information to the relevant individuals. At a minimum, they must be provided with the name of the organization, its purpose or purposes for processing the personal data, and other information necessary to make the processing “fair.” Not surprisingly, this requirement frequently exists in tension with an organization’s desire to conduct the investigation with minimum fanfare and media attention.

- **Legitimate Purpose**: Personal data may only be collected for specified, explicit and legitimate purposes, and may not be further processed in a way that is incompatible with those purposes (this is also known as the “finality principle”). The Directive contains a list of permissible grounds for processing personal data. For organizations processing “sensitive” personal data, defined under Article 8 of the Directive as data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, additional restrictions will apply and the list of permissible grounds is even shorter. Sensitive data can, and often does, include information relating to offences or criminal convictions attributable to an individual, sometimes referred to as “judicial data” by EU authorities.
In most cases, an organization is prohibited from processing sensitive data unless an exemption applies. The most commonly applicable exemptions are:

(i) the individual has given his “explicit” (i.e., informed and freely given) consent (unless national law precludes processing even with such consent). This has been interpreted by most Member States to require actual written consent, rather than merely implied consent;

(ii) the processing is necessary for the purposes of carrying out the obligations and specific rights of the organization in the field of employment law in so far as it is authorized by national law. This will often permit organizations to process personal data about employees and applicants in order to satisfy national labor or anti-discrimination laws; or

(iii) the processing is necessary in order for the organization to establish, exercise or defend itself against legal claims. In the context of investigations, this exemption may be commonly relied upon, although often improperly.

- **Relevance**: Personal data that are collected must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- **Accuracy**: Personal data must be accurate and, where necessary, kept up to date.

- **Retention**: Personal data must not be kept in a form that permits identification of data subjects for longer than is necessary. Organizations are required to make anonymous or delete information as soon as possible.

- **Security**: Organizations must implement appropriate security measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access.

- **Data Transfer**: Personal data can only be transferred outside the EU if the data will receive “adequate” protection in the country where the data are sent. The term “adequate” is not defined in the Directive. However, the European Commission has significant latitude to make so-called “adequacy” determinations regarding the level of protections that a particular country applies to personal data. To date, only a few countries have been found to provide adequate protection -- Switzerland, Canada, Argentina, the Isle of Man and Guernsey. When sending
data to other countries, organizations must consider one of the other available transfer mechanisms – consent of the data subject (a disfavored approach), transfer contracts, Safe Harbor (for US transfers only), binding corporate rules (BCRs), or an applicable exemption. One exemption that organizations frequently consider when transferring investigative data is the exemption that permits transfers “for the establishment, exercise or defense of legal claims.”

Second, the Directive vests rights in the individual data subject. Subject to narrow exceptions, individuals have a right to access any personal data held by an organization relating to them, and to compel the controller to rectify, erase, or block the transfer of any incorrect or inaccurate data. These rights can have interesting consequences in the investigative context, given the ramifications of access to information that could or does implicate an individual in improper conduct. Individuals also can bring private rights of action to obtain compensation for any damage or loss that they suffer as a result of a breach of EU data privacy rules. To date, there have been few civil complaints brought in European courts alleging a breach of data protection rights. Instead, enforcement has largely been the province of national privacy regulators, otherwise known as data protection authorities (DPAs).

C. Data Privacy & Investigations - General Observations

The Directive was not enacted to specifically legislate the collection and handling of personal data in the investigative context, but rather operates at a more general level. And, to date, European DPAs have refrained from releasing much, if any, guidance papers on this subject (as distinct from, say, guidance on workplace monitoring and surveillance), most likely reflecting the fact that this has not, as yet, been a significant priority for national regulators. To the extent that issues have arisen, those appear largely to have been resolved

---

privately. Despite this, there are some provisions appearing in the Directive, and hence in implementing Member State law, that are potentially relevant to corporate investigations, particularly those whose aim is to determine whether a criminal offence has taken place.

Most notably, and understandably from a public policy perspective, the Directive and most national privacy laws relax the application of European data privacy principles where it might jeopardize an organization’s ability to advance or defend itself against legal claims or undermine an investigation or prosecution of a criminal offence, including those occurring in the workplace. Thus, Article 8 of the Directive enables organizations to process “sensitive” personal data -- into which category many Member States would include investigative data revealing an individual’s commission of a criminal offence -- where necessary for the “establishment, exercise or defense of legal claims.” Article 8 also permits organizations to process such data where necessary for the “purpose of carrying out the obligations and specific rights of the controller in the field of employment law,” potentially relevant where one of the motivations underlying an investigation is to ensure compliance with applicable employment or labor laws, such as laws compelling businesses to provide a safe and secure workplace.

Likewise, Article 26 of the Directive allows organizations to circumvent the rules prohibiting transfers of personal data outside the EU where to do so is necessary “for the establishment, exercise or defense of legal claims,” although as noted below questions still persist over the appropriate interpretation and application of this exemption. Article 13, in turn, enables Member States to waive the traditional privacy rules -- including those relating to notice and access -- in cases where personal data are processed for the “prevention, investigation, detection, and prosecution of criminal offences, or of breaches of ethics for regulated professions.” The extent to which these exemptions apply will depend on the facts of each case, and Member States continue to apply and interpret these exemptions differently.
Even so, an organization is unlikely to be able to rely on these exemptions where it engages in a broad-ranging effort to collect personal data, in the form of e-mails, documents and other materials, from its employees based on vague and unsubstantiated rumors that one or more members of staff may have misbehaved; however, it may be able to do so where it gathers personal data about a specific employee that the organization reasonably believes committed a serious criminal offence.

In the former case, the nexus between the investigation and the actual detection of a criminal offence or the assertion of or defense against (still largely speculative) legal claims is too weak for the exemptions to apply. In the latter case, however, the nexus is much stronger, thereby potentially triggering the exemptions. As the above suggests, organizations can expect to more properly fall within the ambit of potentially helpful exemptions to the core privacy rules as their investigations become more narrowly focused on disclosing actual wrongdoing, as opposed to being broad fishing expeditions. And, the argument that these exemptions apply becomes much more plausible where the organization is investigating activities that could constitute serious criminal offences, such as money laundering or accounting fraud, as opposed to investigations aimed at uncovering mere breaches of an organization’s own policies.

Finally, an opening caveat. Organizations conducting investigations need not only consider the implications of their actions under applicable data privacy laws, the principle focus of this paper, but also may need to consider the possible application of other laws -- local employment or labor laws, telecommunications laws, laws protecting correspondence and communications, and Works Council rules, to name just a few. If data are transferred internationally and may end up in the hands of foreign agencies or authorities, national blocking statutes may also be relevant. Although we touch on the above laws at various points in this paper, it is impossible to do them real justice here.
III. INVESTIGATIONS & DATA PRIVACY - IMPLEMENTING PROTECTIVE MEASURES AND EVIDENCE GATHERING

Organizations undertaking an internal investigation are best advised to keep the following maxim in mind -- the application of European privacy rules, and their associated exemptions, will depend upon what kind of investigation is being conducted. At one end of the spectrum, the following scenario can be imagined: an organization wishes to engage in an exhaustive and intrusive review of its staff’s activities and communications to assure itself that no wrongdoing, either by way of a breach of company policy or a more serious criminal infraction, has taken place, simply because management believes this would enhance the company’s reputation. At the other end of the spectrum, another scenario can be imagined, and increasingly is all too real. An organization is faced with credible evidence that certain staff have engaged in serious misconduct that breaches applicable laws, and has no real alternative but to commence an internal investigation of those employees.

The vast majority of investigations that take place today fall between these two extremes. Those that incline towards the first scenario, and that could be characterized as having a wide focus and weak underlying justification, tend to be much more problematic from a data privacy perspective. The full range of EU data privacy rules apply and apply without limitation. By contrast, those investigations that incline towards the second scenario, and that could be characterized as having a narrow focus and strong underlying justification, tend to be much less problematic from a data privacy perspective. In this situation, the data privacy laws, to the extent that they apply, are more accommodating. In this section, we discuss the data privacy implications of what might be termed the “pre-investigative” stage of an investigation. This is the stage immediately before an organization has any belief or knowledge that wrongdoing of any sort has taken place. Today, more and more organizations are pro-actively trying to detect serious misconduct at an early stage or deter it altogether. The most obvious manifestation of this is the increasing prevalence of workplace monitoring,
followed by deployment of hotlines and other mechanisms to allow persons to report improper behavior within the company. However, some companies even demand that their existing and potential business partners furnish information about themselves, including information about staff, to protect themselves against violating applicable laws, such as anti-bribery statutes.

A. Pro-Active Employee Monitoring

Whereas there is a dearth of regulatory guidance on the application of data privacy laws in the context of corporate investigations, the same cannot be said with respect to workplace monitoring. Monitoring, whether it is motivated by a desire to detect or deter potential wrongdoing, protect an organization’s assets, or increase staff productivity, has received a great deal of attention from European privacy regulators both at the national and EU-level. In response to concerns over the increased use of monitoring technologies in the workplace, the highly influential Article 29 Working Party, which comprises representatives from the 27 EU Member State data privacy authorities, issued in 2002 a “working document” entitled “On the Surveillance of Electronic Communications in the Workplace” specifically discussing the data privacy implications of employer surveillance. National data privacy authorities also have published useful guidance in this area, a good example of which is the UK Information Commissioner’s Employment Practices Data Protection Code.

The above guidance -- although not intended specifically to guide organizations about to embark upon a corporate investigation -- remains highly pertinent, and it covers organizations both monitoring employee communications (e.g., e-mail or Internet usage) and employee activities and movements (e.g., CCTV, location trackers and swipe cards). The

---

privacy rules that tend to resonate with particular force in the monitoring context are the following:

- **fair and lawful processing** - ensuring that staff, and potentially third parties interacting with staff are apprised of the organization’s efforts to monitor;
- **proportionate processing** - ensuring that the monitoring represents a proportionate response under the circumstances and does not unjustifiably intrude upon employee privacy;
- **purpose limitation** - ensuring that any data, once shown to be irrelevant to the organization’s investigative purpose, is promptly deleted or destroyed and not used for another purpose;
- **security** - ensuring that any data obtained in connection with a monitoring exercise is held in a secure fashion, and that third parties enlisted to assist the organization are subjected to suitable controls; and
- **data transfer** -- ensuring that restrictions on data transfers outside the EU are satisfied where an organization as a matter of course either allows monitoring to be conducted outside the EU or transmits data obtained via monitoring outside the EU, such as to a non-EU corporate headquarters.

There also are associated issues, such as ensuring that the monitoring comports with local applicable telecommunications laws, which might restrict an organization from monitoring communications to and from staff on the basis that it constitutes an “interception” of that communication. Also, local labor or employment laws frequently restrict an organization’s ability to monitor staff and may require the company to consult with employee representative bodies, such as Works Councils, beforehand.

1. **Maintaining Transparency and Ensuring Openness**

   During the pre-investigative stage, the notice obligation arising under EU data privacy applies in full force. Organizations typically cannot avail themselves of one of the various national law exemptions to the notice requirement, most notably exemptions that permit unnotified processing where necessary to detect or prevent criminal offences or, less
commonly, to advance or defend against legal claims. Because the organization at this juncture has no solid basis for believing that any specific wrongdoing has taken place, the argument that furnishing notice might hinder the detection of (an as yet unknown) crime or hinder the organization’s ability to advance or defend (as yet non-existent) claims is virtually impossible to sustain. Certainly, EU privacy regulators would not be sympathetic to such an argument, and almost certainly would reject it. Further, claims that furnishing notice might not be necessary because it would entail a “disproportionate effort,” yet another familiar exemption to the notice rule, do not appear supportable in the employer-employee context, where delivery of a notice would not require much effort.

Instead, an organization monitoring its employees for purposes of detecting or preventing potential wrongdoing, of whatever sort, more sensibly should consider the appropriate mechanisms for furnishing notice. Regulators have been unanimous in their support for the adoption of clear and detailed corporate policies that inform the workforce about the organization’s monitoring policies with respect to e-mail, Internet and other communications systems, and would expect them to address such topics as the handling of incoming communications while an employee is absent, the status of independent contractors using the company’s communications systems, and so forth. Somewhat more discretionary are the use of additional devices to furnish notice, examples of which include automatic computer pop-ups and warnings that appear on-screen to employees informing them that their communications may be monitored.

The position of third parties, such as family members, friends and others, who communicate with an employee and whose communications may be monitored remains more problematic. Regulators suggest that organizations ensure that standard disclosures appear in all outgoing e-mails, for instance, informing individuals about the organization’s monitoring policies. Of course, this solution is only partial, as it cannot protect persons initiating
communications with staff. Where telephone calls are monitored, a more effective solution is available -- an automated message can be supplied to callers informing them that their calls may be monitored or recorded. At least with respect to incoming e-mails (as opposed to telephone calls where compliance appears to be greater), many organizations today appear to ignore the advice of regulators and thereby run a compliance risk. Judging by their handling of the issue to date, EU privacy regulators do not appear to regard this to be a significant problem, perhaps reflecting the belief that persons transmitting e-mails to a workplace should have a diminished expectation of privacy.

2. Avoiding Disproportionate Data Collection

The proportionality principle, which requires an organization to collect only that amount of personal data necessary to achieve its purpose, requires some thought at the pre-investigative stage. Organizations may rightly wonder what, precisely, proportionate processing entails where pre-emptive monitoring is concerned. The question, unfortunately, does not permit an easy answer. Rather, companies need to engage in a delicate balancing act, weighing the effectiveness of a particular act of monitoring to detect or prevent wrongdoing against the impact it could have upon an employee’s privacy. Finding the right balance will depend on the facts of each case. For example, an organization that reasonably suspects an employee to have bribed a government official should be permitted to engage in a more intrusive examination of that employee’s files or communications; that same effort where an organization only has a vague suspicion that staff may be sending non-work related emails from work would qualify as disproportionate. Moreover, even in the former case, the organization could well be precluded, because it is disproportionate, from opening and
reviewing the suspect employee’s e-mails or files where those show signs of being purely personal in nature.\textsuperscript{9}

At this early stage, regulators evaluating any monitoring activity are likely to be particularly protective of an employee’s privacy rights. Although an organization could quite rightly contend that by reviewing each individual employee’s Internet log files and emails it could more effectively achieve its aim of ensuring the company’s compliance with applicable laws, privacy regulators are unlikely to be persuaded. The harmful impact of such action on individual privacy would more than outweigh -- at this early juncture -- the benefit to the company. For routine monitoring motivated by a general desire to ensure compliance with law or corporate policy, European privacy regulators have expressed a preference for sporadic as opposed to continuous monitoring; review of high-level or aggregate data as opposed to individualized data; review of anonymized data as opposed to personal data; targeted (but justified) monitoring as opposed to blanket surveillance; examination of traffic data as opposed to communication content; examination of purely business-related communications as opposed to non-business communications; and the use of privacy-enhancing technologies (so-called PETs) generally. In fact, the Article 29 Working Party appear to rule out blanket monitoring of employee communications based purely on investigative aims, having noted that “the proportionality principle rules out blanket monitoring of individual emails and Internet use of all staff other than where necessary for the purpose of ensuring the security of the system.”\textsuperscript{10}

\begin{flushleft}
\footnotesize
\textsuperscript{9} European privacy regulators do appear willing to accept that organisations can open the private e-mail correspondence of employees in narrow circumstances, which includes the detection of criminal activity on the part of the employee that affect the interests of the organisation, for example where it could give rise to liability for the organisation or may be detrimental to its business interests. \textit{See}, \textit{e.g.}, Article 29 Working Party, WP 55 at p. 21, fn. 23.

\textsuperscript{10} \textit{Id.} at p.17.
\end{flushleft}
All of this plainly suggests focusing a company’s monitoring efforts upon those business units most likely to raise real compliance issues, for instance its accounting department if compliance with money-laundering regulations is a concern or a procurement function if anti-bribery offences is a worry, and doing so first at a relatively high level to detect anomalies or suspicious activities. And, only after anomalies or activities are detected, engaging in more intrusive monitoring at the individual level. In practice, given the inevitable uncertainty surrounding the proportionality principle and its proper application, privacy regulators are likely to be hesitant to challenge an organization’s monitoring on proportionality grounds alone, provided that an organization can demonstrate a good faith effort to comply.

3. **Ensuring Appropriate Retention and Security**

Where an organization implements a monitoring policy, it will need to ensure that any information, including personal data, obtained as a result of the monitoring are not kept for unreasonably long periods of time and certainly not indefinitely. Usually, breaches of the retention rule are a result of neglect, rather than any intentional desire to retain the information. Organizations are well advised to have in place clear policies and procedures to govern the handling of the information obtained to prevent its inadvertent retention. Establishing the appropriate timeframe often is a matter of good judgment and should reflect facts specific to the organization. A company that amasses a large volume of information from a sizeable workforce legitimately will require more time to conduct a proper review of that information than an organization that collects much less information from a smaller group. Judging by the published guidance papers, a retention period of more than a few months is likely to be viewed with suspicion by regulators, unless backed by compelling reasons. Ideally, and in line with the preference to deploy PETS, the assessment should involve automated processes -- for instance, screening software to detect key words probative
of potential wrongdoing -- to preserve the privacy of inspected communications to the greatest extent possible.

A further complication arises where the organization’s monitoring efforts fulfill several different, unrelated purposes. Those efforts may not only aid or assist in preventing wrongdoing, but the collection of information also may serve useful business needs, such as establishing the facts relating to an ongoing or recent business deal. One purpose might justify holding some of the information for longer, say 12 months as opposed to three. This can be dangerous from a compliance perspective. In these cases, organizations need to consider whether it is possible to redact or anonymize the information prior to 12 months, rather than hold information in its original form as a matter of convenience. Organizations also should ensure that they do not use any information derived from their monitoring for a subsequent, unrelated purpose, as tempting as this might be given the large volume of information that is sometimes gathered. Whether a purpose is related or not largely would depend on the content of the original notices furnished to employees and others.

Finally, it is worthwhile to consider security under this heading. Unlike the later stages of an investigation, where a company may hold information that could incriminate someone and thus the harm that would arise from its inadvertent disclosure is substantial, here the risks are less substantial. Although an organization certainly will have an interest in ensuring that none of the information garnered from monitoring employees is made available to unauthorized persons, EU data privacy laws will permit the organization to adopt measures corresponding to the lower level of potential harm. The more robust measures usually associated with the processing of sensitive personal data -- stringent authentication and access controls, physical and environmental controls and organizational measures -- can be marginally relaxed. As most processing of the information at this point frequently falls within the remit of an organization’s IT department or system administrator, an organization
should apply specific controls that could include confidentiality agreements to the relevant personnel. Where an organization outsources its monitoring efforts to a third party, it will need to implement a suitable data processing contract.

4. **Transfers of Information to Third Countries**

In most cases, organizations engaging in monitoring do not need to transmit the resulting information to a third country. However, in some instances, organizations, particularly affiliates of U.S. companies, may be asked to transfer information to the company’s headquarters or, more problematically, the monitoring is actually conducted by staff located in the U.S. or some other jurisdiction outside the EU. These scenarios implicate the Directive’s prohibition on transfers of personal data outside the EU, and require the organization to consider its compliance options. The Directive’s exemption for transfers “necessary for the establishment, exercise or defense of legal claims” will be unavailing in these circumstances given that the prospect of any legal claim remains remote and entirely speculative. As discussed below in Part V, most Member State regulators will insist that such claims be extant or imminent, and may even refuse to apply the exemption where the relevant legal claims arise before non-EU tribunals, such as those in the U.S. The UK, by contrast, remains somewhat exceptional, as it explicitly allows transfers for “prospective,” as well as pending, legal claims.\(^{11}\)

Rather, organizations will need to consider their options and, traditionally, the most popular compliance solutions tend to be implementing data transfer contracts or, much less preferred, relying on consent. For data transfers to the U.S., if the company’s U.S. operation has enrolled in the Safe Harbor regime for transfers of its human resource information, this remains another option. Each approach carries its own set of advantages and disadvantages,

---

\(^{11}\) Data Protection Act 1998, § 35(2)(a).
and the organization will need to weigh those to determine which option works best for it. The contractual approach probably will involve use of one of the EU’s “model” data transfer agreements and all that those entail: joint and several liability, third party beneficiary rights, and, potentially, vetting by privacy regulators. Consent, in turn, is increasingly disfavored in the employment context, is problematic with respect to third parties whose data are transferred, and can be withheld or revoked at a later time. In light of the possible obstacles, many European organizations sensibly refrain from transferring any data at this early stage, at least until the organization can rely much more comfortably upon available exemptions or the need to export the data becomes more pressing.

5. **Additional Considerations**

In addition to all of the above, there are a host of other potentially applicable laws whenever an organization engages in any monitoring, regardless of the underlying purpose. Where organizations investigate the activities of their staff, and disciplinary or criminal proceedings might later arise, the rights and obligations arising under local employment or labor laws need to be considered. Moreover, the deployment of devices or technologies within the workplace to monitor the behavior of employees to detect potential wrongdoing are likely to trigger obligations to consult or, in some countries, obtain the prior approval of employee representative bodies. However, the need to interact with such bodies typically does not arise where an organization conducts a targeted investigation that is narrowly focused on a limited set of employees.

Additionally, where an organization collects or monitors emails or other correspondence to and from staff from employee PCs or from central servers, then national statutes and constitutional provisions protecting the confidentiality of correspondence become applicable, and distinguishing between, say, reviewing archived emails and emails as yet unopened by an employee can be all that separates a lawful from an unlawful
investigation. And, sitting above all of these various national laws and regulations, at least in Europe, are potentially relevant human rights protections arising under the European Convention on Human Rights and the EU Charter.

B. Inviting the Submission of Probative Information

Instead or in addition to monitoring events occurring in the workplace, many organizations now are implementing tools to elicit information that could prove relevant in uncovering corporate wrongdoing. Although companies have long made use of internal reporting mechanisms, such as hotlines and similar devices, to enable employees or others to report improper, illegal or simply undesirable conduct or activities, the U.S. Sarbanes-Oxley Act has thrust such investigative devices into the limelight. In fact, largely as a result of this U.S. law, the status of internal reporting mechanisms has become hotly contested and highly divisive.

1. Whistle-Blowing Hotlines: Background

The legality of whistle-blowing hotlines and related tools under EU data privacy laws first reared its head in mid-2005, when the French data privacy authority (CNIL) and a labor court in Germany separately examined the question of whether certain compliance hotlines were lawful, and concluded that they were not. In May 2005, two companies, McDonalds France and Compagnie européenne d'accumulateurs (CEAC), notified the CNIL of their intended use of a compliance hotline. In each case, the companies operated hotlines that would allow the submission of anonymous complaints (by telephone or email) regarding possible violations of the companies’ ethical and commercial codes, as well as other

For instance, in the United Kingdom, the Regulation of Investigatory Powers Act 2000 (RIP Act) prohibits the “interception” of a communication in the course of a transmission, which applies to e-mail communications sent or received by employees in the workplace. That said, the RIP Act, and related secondary UK legislation, offer employers a number of potentially broad exemptions and an e-mail communication, once opened, is understood to fall outside the legislation. Other EU Member States, however, have enacted similar laws that equally apply in the workplace, which are construed more broadly, and do not contain such helpful exemptions.
applicable laws, by co-workers. One of the companies cited its obligations under the U.S. Sarbanes-Oxley statute to justify its operation of a hotline. Under that law, covered U.S. companies must implement a confidential and anonymous reporting procedure so that personnel can report “questionable accounting or auditing matters” within the organization.\(^{13}\)

Employee-generated complaints were to be transmitted to and collected in the U.S. Although McDonalds’ hotline was handled internally, CEAC had engaged a service provider to take incoming calls and emails. In order to promote transparency, the organizations had put in place systems so that employees would be informed of any allegations “as soon as possible” in the case of CEAC or two days after any complaints materialized in the case of McDonalds. In addition to concluding that French data privacy law applied to whistle-blower devices principally operated out of the U.S., the CNIL determined that the hotlines would lead to an organized system for reporting alleged SOX violations (and relatedly, the collection of personal data) in a manner contrary to Article 1 of the French data protection statute, which provides that data processing must respect the fundamental rights of French citizens; would increase the risk of false allegations that could damage an employee’s reputation and prejudice him or her; would involve a disproportionate collection and

\(^{13}\) Section 301 (4) of Sarbanes-Oxley states:

(4) COMPLAINTS. – Each audit committee shall establish procedures for –

(A) the receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters; and

(B) the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters.

The Act requires the U.S. Securities and Exchange Commission to ensure that U.S. stock exchanges not list the securities of companies whose internal audit committees do not have appropriate complaints procedures in place. U.S. stock exchanges, in turn, have implemented rules that, for the most part, require compliance with Rule 10A-3 under the Securities Exchange Act of 1934. Rule 10A-3 and Section 10A (m) (4) of the Securities Exchange Act of 1934 reflect the language appearing at Section 301 of Sarbanes-Oxley and call for a confidential and anonymous reporting procedure to be in place within the relevant organisation. See, e.g., New York Stock Exchange Listed Company Manual § 303A.06; NASD Manual § 4350(d)(3); Amex Company Guide § 803.
processing of personal data; and employees referred to in any submitted complaints would not be informed adequately about the use of their personal data or provided an opportunity to oppose their processing.

Shortly after the CNIL’s rulings, a labor court in the German town of Wuppertal decided that the code of conduct of the German branch of the U.S. company, Wal-Mart, violated Germany’s Works Council Constitution Act by calling upon employees to submit anonymous complaints about their co-workers. In the court’s opinion, such codes require Works Council pre-approval because they subject employees to additional obligations (i.e., in this case, employees could be sanctioned for not complying with the code and thus for not using the hotline) and the hotline effectively constituted a means of monitoring employee performance. The court did not assess the legality of the code of conduct, and its hotline provisions, under any other German laws, including German data protection laws. Wal-Mart did not appeal the decision.

2. **Current Status of Whistle-Blower Devices**

Following the French and German decisions in 2005, the topic of internal compliance hotlines generated a great deal of interest among European privacy regulators. Indeed, the Article 29 Working Party released an opinion specifically setting forth its position on the matter in early 2006. In February of that year, the Working Party issued Opinion 1/2006, titled “On the application of EU data privacy rules to internal whistle-blowing schemes in the field of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime” (WP 117), providing much-needed clarification on the legality of compliance hotlines targeting financial and accounting improprieties, including specifically Sarbanes-Oxley hotlines. The Working Party’s prompt publication of its paper following the 2005 decisions in France and Germany underscored its desire to arrive at a harmonized EU approach and avoid having national privacy regulators adopt varying, and
potentially inconsistent, positions. The paper, however, was stated to be “limited to application of EU data protection rules to internal whistle-blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime,” and did not address the privacy issues arising from whistle-blowing schemes generally. The Article 29 Working Party, in more recent exchanges with the U.S. Securities and Exchange Commission, has indicated that it will consider providing additional guidance applicable to other hotlines at their next plenary meeting.\(^\text{14}\)

In WP 117, the Working Party considered the following issues: (i) the legitimacy of whistle-blowing systems; (ii) the application of data quality and proportionality principles; (iii) the provision of information about the scheme; (iv) the rights of accused persons; (v) the security of processing; (vi) the management of internal whistle-blowing schemes; (vii) issues related to international data transfers; and (viii) notification and prior checking requirements. Taken together, the paper now serves as a general guide to organizations operating hotline schemes, although by expressly limiting the paper to schemes with a strong legal basis (e.g., anti-bribery, accounting fraud, etc.), the legality of hotlines lacking a similarly strong legal grounding remains uncertain. Indeed, the concerns expressed by the Working Party about accounting or anti-bribery hotlines are likely to be even more acute with respect to hotlines serving only a general compliance function.

With respect to whistle-blowing schemes, the Working Party offered the following recommendations and observations, among others:

- **legitimacy of whistle-blowing systems:** Whistle-blowing schemes, including related hotlines, whose purpose is to prevent fraud or criminal conduct involving financial

\(^{14}\) Following publication of WP 117 in early 2006, the Article 29 Working Party and the U.S. Securities and Exchange Commission, which oversees compliance by U.S. companies with the Sarbanes-Oxley statute, has exchanged correspondence and U.S. regulators have met with representatives of the CNIL. These discussions produced further clarification on some of the issues raised by WP 117.
accounting or auditing practices, banking activities or bribery may be justified on one of two grounds -- they must be shown to (i) be mandated by a local law (e.g., local accounting or banking laws) or (ii) serve the “legitimate interests” of the organization and not outweigh the privacy rights of individuals. Significantly, and in line with views expressed in earlier papers, the Working Party believes that an organization’s compliance with foreign laws, such as the U.S. Sarbanes-Oxley statute, is not enough in itself to legitimize the use of a hotline in the EU, although it is a relevant factor when assessing whether the organization has a legitimate interest in its operation.

- **application of data quality and proportionality principles:** Hotlines should be structured, whenever feasible, to limit the number of persons entitled to report alleged improprieties and the number of persons who may be incriminated through their use. Hotline users should be actively discouraged from submitting anonymous reports. Moreover, hotlines should be designed to collect relevant information only, and not the submission of extraneous material.

- **provision of information about the scheme:** Employees should be informed of the existence of, purposes served by, and rights associated with a given whistle-blower scheme. The identities of individual whistle-blowers must be held in confidence, provided that the person submits a report in good faith.

- **rights of incriminated persons:** Organizations must inform employees that a report has been submitted accusing or associating them with some wrongdoing, the recipients of any subsequent internal report in which their personal data appears and their rights to access and rectify information appearing in the reports. The Working Party accepts that organizations can curtail these rights where there is a “substantial risk” that the ability to investigate a complaint would be jeopardized as a result of the rights being exercised.

---

15 Following recent U.S. case law, it remains unclear whether the foreign affiliates of U.S. companies need to be invited to participate in Sarbanes-Oxley hotlines. The U.S. First Circuit Court of Appeals, in *Carnero v. Boston Scientific Corp.*, Case Nos. 04-1801 and 04-2291 (1st Cir. Jan. 5, 2006), held that Sarbanes-Oxley does not protect a foreign citizen who reports accounting irregularities at a U.S. corporation’s foreign subsidiary, suggesting the statute (and not just the provision at issue) does not have extraterritorial effect.
• **security of processing operations**: The basic rules on security apply to any personal data gathered when operating compliance hotlines. Where organizations engage service providers, such as call centers, the services contract specifically should address the issue of security.

• **management of whistle-blowing schemes**: Organizations should establish an internal team dedicated to handling whistle-blower reports, such team to comprise individuals specifically trained for the task and to be separate from other corporate departments, such as the HR department.

• **transfers to third countries**: Where personal data collected in the course of operating an EU compliance hotline are transferred outside the EU, for instance to an organization’s corporate headquarters, then a mechanism for complying with EU transfer rules must be in place.

• **notification requirements**: Finally, organizations must comply with national rules on notification, to the extent those cover compliance hotlines. In some cases, such as in France or the Netherlands, prior authorization from (and not simply notification to) privacy regulators also may be required.

Although the Working Party opinion paper does not enjoy the force of law and so is not directly binding on organizations processing personal data in the EU, the strong presumption following publication of WP 117 is that if an organization fails to comport with its recommendations, it will be in breach of national EU data privacy laws. Organizations that maintain and operate their European compliance hotlines in a contrary manner undoubtedly run a greater compliance risk, unless they can point to more permissive national level rules, guidance or decisional case law. That seems unlikely and a number of national regulators, such as the Dutch, Belgian and Irish, already have published papers conforming to the views expressed in WP 117. Thus, organizations operating compliance hotlines of any sort in the EU should consider modifying their hotlines to respond to these legal developments.
Already, it appears that a number of multi-national firms are radically overhauling their hotline reporting structures so that reports arriving from EU jurisdictions are distinguished and afforded separate treatment. For some organizations, modifying existing hotlines may prove impracticable to achieve in the short term or expose the organization to potential liability under other regulatory regimes that appear to mandate the use of non-compliant hotlines. In that event, it may be necessary to decide whether the operation of a particular hotline, possibly to comply with other applicable regulatory requirements, should take priority over compliance with EU data protection rules. In making this determination, the organization will need to weigh the financial penalties arising from a breach of the EU data protection laws, along with the reputational implications of non-compliance, against the potential fines and sanctions that non-compliance with other regulatory obligations could entail.

C. **Due Diligence Involving Third Parties**

Besides pro-active employee monitoring and implementing hotlines and other whistle-blower mechanisms, organizations are increasingly conducting due diligence of their existing and prospective business partners. Principally, these efforts are driven by fears that the company may inadvertently collaborate with third parties whose business conduct may implicate the company in wrongdoing. The nature of the due diligence can take varying forms and involve differing degrees of intrusiveness. On the one hand, it can involve requests that business partners complete questionnaires or applications about their own business practices, management structure and business ethics. On the other hand, and more problematically, some organizations may feel that in order to obtain worthwhile information their efforts need to be covert and possibly involve professional investigators trained in conducting corporate due diligence. Although frequently the information gathered is not personal, it can be. It may involve background checks to determine if business partners
previously have been convicted of criminal offences or have engaged in fraudulent business practices. It may even involve gathering information on a business partner’s family members and business associates, with or without the knowledge of the relevant persons.

1. **Maintaining Transparency of Information Collection**

EU privacy rules dictating that the processing of personal data be open and transparent, and involve the delivery of appropriate notices, can cause issues where an organization performs extensive due diligence on actual or potential business partners. Most clearly, an organization that wishes to ensure that its efforts remain covert is likely to run into significant problems. Unless a business has some well-founded belief, or at a minimum a strong suspicion, that its existing or potential business partner is breaching criminal laws, then reliance on one of the exemptions to the traditional notice requirement seems highly dubious. Upon learning that a company engages in covert due diligence as a matter of routine, most European privacy regulators almost certainly would question the failure to provide appropriate notices to any individuals whose personal data are captured in the absence of any clear legal mandate permitting such unnotified processing.

As is the case of routine employee monitoring, efforts to justify unnotified due diligence on the basis that it is required to “prevent, investigate, detect or prosecute criminal offences” or, for regulated professions, breaches of applicable ethics rules will likely prove unavailing given the remoteness of any actual offence. Where an organization actually begins to suspect wrongdoing (and this scenario most likely would only apply to existing, not potential, business partners), then the above exemption might prove relevant. Further, claims that furnishing notice would require the company to engage in a “disproportionate effort” look vulnerable and difficult to sustain, particularly given the scepticism with which such claims are viewed by European privacy regulators and the implications for the relevant individuals in case any potentially incriminating information is found. Rather, barring
extraordinary circumstances, organizations engaging in routine vetting of their business associates will need to take care to ensure that appropriate notices are furnished. What is more, where these efforts extend to the point where detailed background checks are performed on individuals, which would result in the collection of sensitive personal data (e.g., criminal offences), then it probably will be necessary to secure prior consent -- this assumes, of course, that such efforts will not be struck down on proportionality or other grounds.

Even where the organization intends to be entirely transparent about its information gathering practices, difficulties can still arise. Increasingly, organizations are asking that all of their potential business partners complete and return a detailed questionnaire or application that will reveal information not only about the applicant, but the directors and officers of the applicant’s company and even their family members. For instance, this may be done in order to determine whether any individual has an improper relationship with a government official that could be indicative of corrupt business practices. The organization may be quite happy to let the applicant know that this is the purpose served by the questionnaire or application, but encounters difficulty in getting this message to everyone else whose information will appear on completed forms. Here, the notice rule can prove challenging to satisfy as the organization has no relationship with these third parties, and no efficient mechanism for delivering notice. While the temptation here to assert a “disproportionate effort” defense will be strong, and could prove persuasive to regulators in the right circumstances, it leaves the company potentially exposed in the event a regulator ultimately disagrees. In the end, if the organization is committed to this approach, it may be obliged to compel persons submitting the questionnaire or application to furnish notice on the organization’s behalf, not particularly ideal or conducive to harmonious business relations.
2. **Avoiding Disproportionate Collection**

When gathering information on business partners, organizations need to be attuned to the proportionality principle as a good faith effort to conduct reasonable due diligence may quickly spiral into something more comprehensive and intrusive. This can be a particular risk where the due diligence process is outsourced to third parties, such as professional investigators, without any regard to the methods to be employed. As noted above, particular difficulties can be expected where background checks are performed and information solicited from, say, criminal records bureaux, court records or other information sources that might disclose whether a business associate has a criminal past. Without the benefit of a local law permitting or requiring such a privacy-intrusive activity, organizations may be required to obtain the relevant individual’s consent first to perform such checks. Even assuming such consents are forthcoming, it still may prove difficult to show that such checks represent a proportionate response in light of the perceived commercial or legal risks faced by the organization. This would need to be assessed on a case-by-case basis, taking into account various factors, such as support for such efforts arising under local laws or the effectiveness of such checks in preventing the company from engaging in unlawful conduct.

3. **Transfers of Information to Third Countries**

Finally, problems can be raised where the company -- once it completes its due diligence -- intends to communicate the results to affiliates outside the EU or even foreign agencies and authorities. These scenarios thrust the data transfer rule front and centre. Again, as with transfers of information pulled from employee monitoring efforts, arguing that the transfers should benefit from one of the exemptions to the transfer rule -- such as to detect or prosecute a criminal offence or to advance or defend legal claims -- will be a challenge. Ignoring the fact that the information only may reveal possible, not actual, offences or that any legal claims have not yet materialized, EU privacy regulators will feel particularly
uncomfortable where the offences or claims in question are associated with the foreign jurisdiction. Take the example of a U.S. parent requesting that its French affiliate send information about all potential business partners to determine whether they represent a risk under the U.S. Foreign Corrupt Practices Act (FCPA). The CNIL is unlikely to find on these facts alone that the company may be eligible for one of the above exemptions to the transfer rule. In fact, in informal discussions with European regulators about this scenario, some have expressed grave reservations about FCPA-backed due diligence activities more broadly. The analysis might change, however, where it becomes evident that an FCPA breach may have occurred and the information will be sent in order to enable a company to prepare its defense in a prosecution or investigation brought by the U.S. Department of Justice.

Even here, the situation is not entirely clear, as some have maintained that the legal claims and detection and prosecution of offences exemptions to the transfer rule need to relate to claims or offences arising in the EU, not a foreign state. This interpretation of the law has been bolstered by an Article 29 Working Party document, WP 114 entitled “Common Interpretation of Article 26(1) of Directive 95/46/EC,” and discussed below. So, in the above example, if the U.S. Department of Justice issues a broad-ranging subpoena to the company’s U.S. office requesting information, some of which is held by the French affiliate, the French affiliate still will need to consider its options carefully before jumping to the conclusion that any of the above transfer exemptions apply. There also may be local blocking statutes, which restrict disclosures of certain information to foreign tribunals and regulators, that may need to be considered. To avoid the difficulties arising in such cases, some organizations even have asked to be compelled by local government authorities, law enforcement or courts to comply with the overseas law enforcement request, which then offers a much more secure basis for transferring the data in a manner that comports with EU data privacy law.
IV. INVESTIGATIONS & DATA PRIVACY - CONDUCTING WIDE-RANGING INVESTIGATIONS INTO POSSIBLE WRONGDOING

We now turn to consider the data privacy issues that arise once the investigation further matures and reaches the point at which an organization has some well-founded belief that a person or persons within the organization is or has acted improperly or unlawfully. We move from the realm of due diligence and prophylactic measures to the situation where there is now a probability that some undesired conduct has taken place, whether it be sexual harassment, theft of corporate assets, tax or accounting fraud or bribery of public officials. It may even be the case that the company has learned, either directly via compliance hotlines or from law enforcement officials, that particular employees or third parties have behaved wrongly, and is now attempting to ascertain the full extent of the problem. At this stage, the company may decide that it is prudent to engage third parties to facilitate the investigation and to lend it an air of impartiality. Whatever the circumstances prompting the inquiry, a thorough and intensive investigation is likely to be the company’s only option.

From a data privacy compliance perspective, this can be the most challenging phase of an investigation, as the application of potentially helpful statutory exemptions -- for instance, exemptions to the notice rule or the transfer prohibition -- may be decidedly unclear and a company will be strongly tempted to avail itself of those exemptions to identify wrongdoers. These exemptions are intended to relax the customary application of key data privacy rules where that would interfere with the investigation and detection of persons engaging in criminal acts or prevent an organization from asserting its rights or mounting a proper defense to a legal action. And yet, a company may question whether providing notice to personnel whose hard drives are to be scanned and reviewed would, in actual fact, prejudice the investigation of a criminal offence where it remains uncertain whether an offence actually has been committed; whether it is appropriate to refuse access made by staff on similar grounds; and whether the transfer of accumulated data to external legal advisors
really would enable the company to advance or defend against legal claims where such claims are likely, but not a certainty.

1. **Maintaining Transparency and Competing Considerations**

As noted already, EU data privacy laws require organizations to ensure fair and transparent processing of personal data, which typically entails the provision of a suitably detailed notice to the relevant individuals. We have seen how, when monitoring employees or gathering information on business partners, organizations will have little option but to furnish notice about their activities, often relying on internal policies (for employees) and other mechanisms to provide notice. Even at this more developed stage of an investigation, organizations generally should furnish notice to staff, as reliance on exemptions, notably the notice exemption relating to the detection or prosecution of persons involved in criminal offences, is laden with risk. Although there may come a point later when the organization may need to consider whether this exemption applies, for instance when the investigation becomes more narrowly focused on specific individuals, it ordinarily will not apply at this juncture. The investigation most probably will not and cannot be conducted covertly, and so staff will know about these investigations in any event, as they will need to act on litigation holds, hand over files and documents or make their computer equipment available for scanning. Accordingly, a company will spend its time more profitably considering not whether to notify employees, but how and when. The company may have generally advised staff in the past of the need to process their personal data for general “investigative” purposes or to “protect the company’s interests,” but this language may be too imprecise to discharge effectively the company’s notice obligation. And, if third parties, such as legal counsel, are involved in gathering files and information, it is best to explain who they are and where they fit in the investigation, if only to encourage employees to cooperate with them.
Rather than a burden, an organization more positively should view furnishing notice as an opportunity to manage the fears and concerns of the relevant staff, some of whom may be distressed to find themselves embroiled in an internal investigation. Companies may wish to supply employees with a separate notice in writing and have them acknowledge receipt. As an evidential matter, this is the preferred approach. Less preferred, organizations may look to rely on oral disclosures, although in certain jurisdictions that require written disclosures like Germany this may not be possible. It will want to ensure that whichever method furnishing notice is adopted, the risk of disclosure to third parties unconnected with the investigation, and the potential reputational damage that this could cause, is kept to a minimum. The paramount consideration is that the relevant individuals are notified, ideally before the company collects any personal data, and are able to raise any concerns that they may have. For investigations spanning multiple jurisdictions, national law variations on the notice requirement may need to be taken into account. In the UK, for example, the Information Commissioner has adopted a fairly flexible and open standard. By contrast, French and Italian data privacy laws impose much more onerous requirements in terms of the information that a notice must include.

Although the position with respect to notifying employees may be relatively clear, the position with respect to third parties is often less clear. Almost invariably, wide-ranging investigations, where files, corporate documents, meeting minutes, electronic communications, and other materials are gathered, involve the collection of personal data relating to third parties. These can range from business contacts of the company, who may also have reason to fear investigation and possibly prosecution, to friends and personal contacts of employees. Here, the company needs to consider its position carefully. In certain scenarios, the Directive’s “disproportionate effort” exemption may well offer some relief. For example, assume a company scans the hard drives, including received and sent emails, of
employees in its procurement department. It likely will be the case that some captured emails will contain personal data relating to third parties, many of whom are entirely irrelevant to the investigation. Privacy regulators may be persuaded by a company’s claims that to require it to notify all persons, even those of no consequence to the investigation and whose personal data will be disregarded, entails a disproportionate effort.

Again, companies will need to be mindful of national variations in this regard. In some countries, like the UK, an organization itself will be able to assess whether the burden is “disproportionate,” while in others, like Italy or Spain, local privacy regulators first will need to be consulted. This assumes, of course, that the data qualifies as personal data in the first instance. At the threshold, an organization will need to determine whether the information at issue qualifies as protected personal data. The Article 29 Working Party adopted a broad interpretation of the term “personal data”16 in WP 136 and certain Member State regulators have since issued national guidance to ensure consistency with the Working Party’s approach. The UK Information Commissioner, for example, recently issued guidance indicating that information will be personal for purposes of the Directive where it is “obviously about” or “clearly linked” to an individual. This interpretation is a significant revision to the Information Commissioner’s previous, and narrower, interpretation of the term and largely follows the wider approach taken by the Working Party.17 EU Member States seem inclined to adopt more expansive interpretations of the term personal data as technology advances. As a result of this, organizations involved in investigative activities are unlikely to be able to avoid the notice question.

Nevertheless, other scenarios where the privacy interests of the third party are implicated to a greater degree also are possible to imagine. For instance, certain third parties whose personal data are collected in the course of scanning employee hard drives later may become implicated in the investigation or may be believed to be key figures at the outset. For these persons, furnishing notice, although entailing some cost and effort, may not entail a “disproportionate” effort given the adverse impact that the investigation may have on the privacy interests, and possibly other interests, of the individual. This may not only be a matter of data privacy, but also due process and fundamental fairness where individuals are exposed to potential civil or criminal liability. The difficulty for organizations will be deciding at what point the notice requirement has been triggered, taking into account numerous factors such as the extent to which the individual is implicated by the investigation, the level of harm to which the individual may be exposed as a result of the investigation, and the time and effort required to locate him or her. However, and somewhat perversely, once the individual is clearly identified as a potential suspect, a company then may need to consider whether a further notice exemption applies -- the exemption that applies when furnishing notice would prejudice the detection or prosecution of a criminal offence.

2. **Ensuring a Legitimate Basis Exists**

As a matter of EU privacy law, an organization collecting and processing any personal data during an internal investigation must ensure that this qualifies under local law as a “legitimate” data processing exercise. This in itself raises the question of whether the personal data collected during an investigation will be “sensitive” personal data -- under the laws of some Member States, including the UK, information relating to the alleged commission of an offence will be deemed sensitive -- or mere personal data. At this stage of an investigation, where a company is likely only have a general suspicion, and no hard proof, that any person or persons have committed an offence, there are strong grounds for
contending that the information collected falls under the non-sensitive rubric. Gradually, as more evidence of wrongdoing is gathered and suspicions harden into actual knowledge that an offence has been committed, the data could convert into sensitive data.

That said, guidance released by the Article 29 Working Party suggests that some regulators, at least, are willing to adopt a broad construction of the notion of sensitive data in the investigative context. In a 2005 “working document,” the Article 29 Working Party controversially concluded that IP addresses collected and processed by rights holders simply when monitoring the Internet for evidence of possible copyright infringement are not only personal data, but specifically sensitive “judicial data” (i.e., “data relating to offences, criminal convictions or security measures”). In some EU Member States, this result would give rise to an obligation to consult, and perhaps obtain the approval of, regulatory authorities. And yet, in the Working Party’s more recent paper (WP 117) on compliance hotlines discussed in Part III, it appears to embrace a narrower conception of the term sensitive data, as it relates to information concerning criminal offences. There, the Working Party considered the possible legal bases for collecting and processing personal data furnished via a company compliance hotline, which arguably is more directly associated with the commission of a criminal offence than IP addresses collected by rights holders, and significantly looked to Article 7 of the Directive, which lists the permissible grounds for

19 The Article 29 Working Party’s view remains controversial. Early drafts of the Directive, and the Article 8 text that refers to “data relating to offences, criminal convictions or security measures” in particular, suggest that provision was intended to allay concerns about the possible misuse by private parties of records or data arising from formal judicial or administrative proceedings. Only later was this language expanded into its current formulation. In other words, the drafters of Article 8 did not intend for it to inhibit organisations from engaging in legitimate efforts to detect whether certain individuals are engaged in criminal conduct that could adversely affect their own interests. Rather, it was intended to limit the extent to which private parties could use information or records relating to an individual’s commission of an offence in light of the highly prejudicial nature of that data.
processing non-sensitive data. In doing so, the Working Party implicitly appeared to accept that such data would not be sensitive personal data as a matter of EU data privacy law.

In light of the above, the precise tipping point at which investigative data will “relate to” the commission of an offence, such that it then becomes sensitive personal data, is likely to be unclear and regulators themselves may well disagree. Broadly speaking, in the initial stages of an investigation where the organization largely is gathering materials and conducting a threshold review to assess relevance, it should be possible to contend that the organization is processing only non-sensitive personal data, and need only demonstrate a corresponding legitimate ground. Ordinarily, there should be little difficulty in justifying the investigation and associated processing of personal data at this early stage either on the basis that the inquiry serves the legitimate interests of the business (e.g., to ensure clean accounting practices, prevent fraud or recover misappropriated assets) or on the basis that the investigation and retrieval of data are necessary to comply with a legal obligation to which the company is subject (e.g., compliance with anti-terrorism legislation, money laundering regulations or health and safety at work regulations).

However, once the investigation becomes focused on particular persons and evidence of wrongdoing begins to accumulate, such that the commission of a criminal offence becomes not just possible but probable, the organization will need to consider whether a legitimate ground for processing sensitive personal data exists. It may only take a matter of days or even hours to reach this point in the investigation. Where the offence in question arises under local laws, organizations often can legitimize their continued processing as necessary for the “establishment, exercise or defense of legal claims,” as the offence frequently will expose the company to potential litigation brought by third parties and/or will require it to assert claims against either the employee(s) or third parties. As we discuss in Part V, an added complexity is created when the offence and any associated claims arise under the laws of a non-EU state,
for instance U.S. laws, or where a company is seeking to comply with a court order or document production request from a non-EU authority. Some EU privacy regulators take the position that it would be improper for a company in the EU to collect and disclose personal data to its non-EU parent under these circumstances.

3. **Avoiding Disproportionate Data Collection**

Whenever undertaking a corporate investigation, a company will need to be careful to avoid collecting an excessive, or disproportionate, amount of personal data. An organization can quickly fall into the trap of disproportionate collection, especially when exposed to intense pressure from a parent company or external regulator to go to any and all lengths to find the guilty parties. At this point, it is useful for the organization to consider what, ultimately, it hopes to achieve when setting the parameters of the investigation and deciding its scope. An organization investigating possible breaches of a minor corporate policy, for instance the company’s Internet-use policy, will not be permitted to intrude upon its employees’ privacy to the same degree as if it were investigating the commission of a serious criminal offence.

Even in the latter case, there are some types of materials, such as plainly personal documents or email correspondence, whose collection and review will be regarded as disproportionate by most privacy regulators unless it can be shown that the items in question are material to the investigation. Indeed, measures need to be in place to prevent staff or external third parties assisting in an investigation from gathering or reviewing data that are clearly personal and irrelevant to the investigation, bearing in mind that some of the material may be sensitive data. For example, emails pulled from an employee’s computer may show that he is taking a prescription medicine, thus disclosing a health condition. Companies should provide personnel or third parties reviewing materials and documents with clear instructions on how they should handle data, including personal data, that are clearly
unrelated to the inquiry. Further, it is prudent to ask persons involved in any review to sign a confidentiality undertaking, which not only enhances the level of security but also keeps reviewers focused upon relevant investigative data.

In this regard, some data collection exercises can be particularly troublesome. For instance, simply scanning an employee’s hard-drive, without first distinguishing between work-related and personal files, could be problematic. Some regulators now encourage employers to allow their employees to be on hand when computers are scanned or files copied to help ensure that only potentially relevant files and materials are obtained, and that purely personal materials are excluded. It also would be improper to obtain materials that plainly fall well outside the relevant period under investigation. If, for instance, there is reason to suspect some wrongdoing took place in 2004, then the relevant materials reviewed should correspond to that time period, unless there is good reason to believe that extending the review more broadly would generate useful evidence. And, the company should select with care the relevant persons who will fall within the ambit of the investigation. The temptation may be to include everyone, and then sort the guilty from the innocent. Almost invariably this is the wrong approach, and it is much better to focus upon those particular departments or divisions within the company whose personnel are most likely to have engaged in the alleged conduct being investigated.

4. **Ensuring the Security of Gathered Data**

As the investigation progresses, and the company begins to amass large quantities of information, thought must be given to ensuring compliance with applicable security rules. EU data privacy laws require that any personal data are afforded adequate protection throughout the life of the investigation and for as long as data are subsequently retained. The methods used both for gathering information and ensuring its availability to reviewers has become increasingly sophisticated of late, reflecting the multitude of document management
technologies on the market. Fewer and fewer companies are simply putting investigative materials into boxes, placing them in a dedicated “data” room and then making this room available to reviewers, whether it be the company’s own staff or those hired to assist in the investigation. Instead, companies are making good use of virtual data rooms, electronically scanning documents and materials and then supervising access to the “room” by establishing authorized users and implementing access controls.

Virtual data rooms plainly offer some advantages over traditional methods of managing document-gathering exercises, although they are not without their own unique risks. On the one hand, the company can control access to gathered information by assigning unique IDs and passwords to authorized users, auditing use of the room to prevent or detect potential security breaches, and allowing access to materials on a read-only basis. By allowing parties in multiple locations to access the data, it also avoids the security risks associated with some of the more traditional methods for transmitting information (e.g., faxes or post). On the other hand, any information kept in electronic form remains vulnerable to some degree, whether it be from persons seeking to hack into the “room” or reviewers failing to keep their IDs and passwords confidential. If a company opts for a traditional room to store its documentation, that room should be physically secure and access to it strictly regulated. As noted above, persons reviewing any materials should be asked to sign a confidentiality undertaking and forbidden from removing materials, a frequent temptation.

Closely related to the question of security is the question of the status of lawyers, auditors and other third parties that may be called upon to assist in the collection and evaluation of data. Some have contended that lawyers and independent auditors are positioned, in data privacy terms, as co-controllers with respect to the information they are called upon to review, reflecting the fact that they often are subject to independent legal, ethical and professional rules when handling the data. Others, however, take the view that
these parties are mere processors acting on the company’s behalf because they have been hired to assist in the investigation, and as such companies should subject them to sufficiently rigorous data processing contracts. On this precise point, the law remains unsettled, and clarifying regulatory guidance from national privacy regulators has not been forthcoming. So, today, disputes still occasionally erupt between a company’s in-house counsel and external advisors over whether a data processing contract should be in place. Given this uncertainty, and subject to further clarifying guidance from national regulators, companies at least should require their external advisors to commit to a robust confidentiality undertaking, which fulfils some of the aims underlying traditional processing contracts.

5. Handling Requests to Access Data

Increasingly, European residents are becoming aware of their data privacy rights, and this has led to an upsurge in subject access requests, both in the investigative and other contexts. The Directive grants individuals a right to request information about their personal data and a right to request rectification or erasure of incomplete or inaccurate data. One of the most difficult issues a company can face during the course of an investigation is what to do when confronted with such requests. In most cases, a company will be tempted to refuse such requests outright fearing that it may somehow compromise the investigation or is an unnecessary distraction. But, unless the request is blatantly abusive, the company cannot turn a blind eye. In any period prior to the investigation and while the company holds only a general or vague suspicion that an employee or employees may have been involved in wrongdoing of some sort, an exemption that allows organizations to refuse access because it would prejudice “the prevention, investigation, detection and prosecution of criminal offences” will not apply, even assuming it is found in the applicable local privacy law. This could change, however, once the investigation becomes narrowly focused upon one or more employees who are believed to have committed a crime.
At this stage of an investigation, however, the company should be prepared to accede to such requests, bearing in mind that EU Member States impose differing deadlines for complying with them. In the UK, a company will need to respond within 40 days, whereas in Spain, for instance, the company will have 10 days to respond. For most EU Member States, the relevant time period for a response tends to fall somewhere between 20 and 40 days. Failing to observe these strict deadlines easily could give rise to breaches of applicable data privacy laws. That said, a company will want to avoid any inadvertent disclosure of information that could be potentially disruptive to the investigation or that might reveal personal data relating to third parties, and accordingly should implement some procedures for vetting and approving (or denying) such requests on a timely basis. It thus is sensible for a company to designate at the investigation’s outset a particular person or persons to manage such requests, in the event that they do arise.

6. **Considerations Related to Transferred Data**

What should a company think about, from a data protection perspective, if it elects to transfer personal data abroad to a member of the corporate group or third parties? Where the data are being transmitted within the EU, this should raise fewer compliance issues. However, the transfer of information to a corporate parent or affiliate in a non-EU country is an entirely different matter. As an investigation progresses, the pressure applied by a corporate headquarters or a foreign regulator may become overwhelming. The first question the company should ask itself is what is the country of the data’s destination and does that country provide an adequate level of protection for personal data? In cases where the country of destination is not one of the few to date to have benefited from a European Commission “adequacy finding,” the company sending the data will need to ensure a mechanism is in place for the safe passage and, post-transfer, the limited and secure handling of the data. Alternatively, the company may consider relying on exemptions to the transfer prohibition
that permit exports of data to detect or prosecute a criminal offence or to advance or defend against legal claims. As noted below in Part V, reliance on these exemptions can be problematic and, in any event, they generally are not applicable at the outset of an investigation.

At this stage, one method of complying with the EU’s transfer prohibition is to anonymize all data prior to its overseas transfer. This involves deleting all names and other identifying information in the gathered material prior to its transfer, which can be a labor-intensive process. This approach may not always succeed, however. It is clear that some EU privacy regulators ascribe to the “objective” theory of personal data, pursuant to which data are “personal” provided that someone, somewhere (here, the EU affiliate) is able to attribute the data to a living person. Moreover, seeking to anonymize the information may be a non-starter where the overseas recipient needs to review the information to discover which individuals are involved. In short, anonymization may not be conducive to an effective due diligence exercise, as employee associations and relationships can be very revealing and may be an important element in identifying any perpetrator within the organization.

Where anonymization is not an option, for whatever reason, another option is to put in place a suitable data transfer agreement, such as one of the EU’s model contracts. These agreements will oblige recipients of any data to implement and maintain technical and organizational controls over the personal data. This approach may work fine when transmitting information to a company’s headquarters, since the transfer is made between two affiliated organizations and contractual disputes are unlikely. It is less practical when the recipient is an unrelated third party, such as a local regulator, which may be unwilling to enter into a binding contractual relationship with the EU company sending the data. Not surprisingly, here a company may find itself with limited options. Although there are always the prospects of obtaining employee consent, European privacy regulators are unlikely to
react well to such an approach, given underlying concerns about the inherent coerciveness of the employer-employee relationship.

V. INVESTIGATIONS & DATA PRIVACY - TARGETING SPECIFIC INDIVIDUALS BASED ON CREDIBLE INFORMATION

We turn now to where an investigation has matured to the point that the company can focus upon suspected wrongdoers. Here, the company no longer is engaged in a broad information-gathering exercise, but is reacting to credible information that certain employees or third parties are involved in inappropriate or unlawful activities. Among other things, the company will be concerned to ensure it can effectively secure evidence of the wrongdoing without giving the suspect an opportunity to cover his or her tracks, for example, by erasing potentially incriminating evidence from his or her computer hard-drive or destroying relevant paper files. From a data privacy perspective, the laws now may begin to shift slightly in the company’s favor, at least insofar as the company may -- at least in some EU Member States -- rely upon exemptions to the core data privacy rules designed to protect a company’s legal interests and facilitate the detection and prosecution of criminal activities.

That said, it is not all plain sailing at this stage. Less helpfully, the data collected and processed by the company are more likely to qualify as sensitive personal data, as they now will relate much more closely to the commission of an offence. Processing of such data is likely to be subject to more stringent rules relating to security and legitimate processing as a result. And, special, and often intractable, problems are likely to arise at this juncture where a company’s investigation is carried out to detect violations of foreign, not domestic, laws, as there will be some question as to whether the above exemptions apply. Some, perhaps most, EU privacy regulators are likely to conclude that they do not, leaving the company in a difficult position trying to respond to the demands of an overseas parent, regulator or tribunal on the one hand, while complying with applicable EU data privacy laws on the other.
1. **Withholding Notice to Relevant Parties**

Once the investigation focuses upon particular individuals, and there are good grounds for believing that they have or are committing criminal acts, the organization may wish to avail itself of the exemption to the notice rule for the “prevention, investigation, detection and prosecution” of criminal offences. Of course, this exemption will be of limited or no use where the conduct investigated amounts to a mere breach of corporate policy. However, for more serious behavior that constitutes a criminal offence, the exemption may now apply, although it may be the case that the individual previously was notified at an earlier stage of the investigation. The basic purpose of the exemption is to avoid the destruction of potentially probative or incriminating evidence that might arise from furnishing notice, and therefore to invoke it properly a company should be prepared to show that such destruction remains a credible risk. In WP 117, the Article 29 Working Party discussed this exemption and explained that:

> where there is substantial risk that such notification would jeopardize the ability of the company to effectively investigate the allegation or gather the necessary evidence, notification to the incriminated individual may be delayed as long as such risk exists. This exception…is intended to preserve evidence by preventing its destruction or alteration by the incriminated person. It must be applied restrictively, on a case by case basis, and it should take account of the wider interests at stake.²⁰

By using the term “substantial,” the Working Party plainly wanted to dissuade companies from using the exemption as a pretext for withholding notice unnecessarily. Whether a “substantial” risk exists likely will reflect a number of factors, such as the nature of the evidence (i.e., whether it is susceptible to quick destruction) and an individual’s ability to gain access to it either directly or through others. In practice, a company and regulators could

---

²⁰ Opinion 1/2006, titled “On the application of EU data privacy rules to internal whistle-blowing schemes in the field of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime” (WP 117).
end up disagreeing whether there is a “substantial,” as opposed to marginal, risk that furnishing notice will jeopardize an investigation, although it is hoped that regulators will afford companies some margin of discretion.

Companies relying on the exemption also will need to bear in mind a few additional considerations. First, Member States do not all apply the exemption in a consistent fashion, and some may not even apply it at all. Whereas the exemption arises under UK law, it does not appear in the German or Belgian data protection laws. And, in France, it is generally invoked by public, not private, bodies. Where local data privacy laws do not contain the exemption, organizations will need to consider whether, in the alternative, they can sensibly rely on prior notices furnished to staff. Although these disclosures by necessity have to be general in nature, for instance informing employees that their data may need to be processed by the company “to protect its legal interests” or “to investigate violations of the law,” they still may offer some degree of protection. Regulators in practice should be sympathetic to a company’s well-grounded concern that in providing notice they may undermine an ongoing investigation. Second, even where the exemption may be invoked, there will likely come a point in time where the provision of notice will not prejudice the prevention or detection of the crime or the identification of the offender, simply because the offender has been identified and the company has secured sufficient evidence relating to the offence. Accordingly, a company relying on the criminal-offence exemption will need to continually assess whether the circumstances of the investigation have changed so as to warrant furnishing belated notice.

2. **Ensuring a Legitimate Basis Exists**

If a company has a reasonable suspicion that a certain individual is involved in a criminal act, it is likely that by investigating that individual and gathering what are likely to be incriminating documents, the company will be handling sensitive personal data and may
How can the company justify the collection and subsequent processing of such sensitive information? There are two exemptions that the organization will want to explore. First, organizations can process sensitive data where necessary for the “purpose of carrying out the obligations and specific rights of the controller in the field of employment law,” potentially relevant where one of the motivations underlying an investigation is to ensure compliance with applicable employment or labor laws, such as laws compelling businesses to provide a safe and secure workplace. To illustrate: suppose an employee accuses another employee of harassment and lodges a complaint with senior management. By failing to respond to the accusation and conduct a thorough investigation, the company may breach its statutory duties. Accordingly, prompted by the complaint, the company launches an investigation into the claim. By doing so, the company is processing sensitive personal information because harassment is classed as an offence under local law. At the same time, there is justification for the processing -- by collecting information necessary to substantiate the allegation, the employer is acting in accordance with their legal duty to ensure a safe and secure workplace free of harassment.

Second, organizations often may process sensitive personal data where necessary for the “establishment, exercise or defense of legal claims.” In the UK, where the exemption also expressly covers prospective claims, it may, for example, apply where an employer fears that an employee who has suffered abuse at work will take legal action against the company for breach of its implied duty to provide a safe and harassment-free work environment. The UK is, however, atypical and in other Member States the claims may need to already exist or be imminent for the exemption to apply. It remains unclear, for instance, whether it is proper

21 Where the conduct investigated does not constitute a criminal offence, but does amount to a breach of an internal corporate policy, the information should not be regarded as “sensitive” in nature. In this case, processing arguably could be justified on the ground that the investigation serves the legitimate interests of the company.
to invoke the exemption where there is only a likelihood of claims arising or where it is not in the company’s own power to bring legal claims but would require the involvement of external regulators or law enforcement bodies. If, for example, an employee is investigated for contravening money-laundering laws, a company may rightly wonder whether the legal claims exemption is available to it, as opposed to the law enforcement bodies actually tasked with prosecuting infringers.  

A further, troublesome scenario arises where an EU affiliate of a company whose headquarters are outside the EU commences an investigation to detect infringements of foreign -- generally U.S. -- laws that apply in an extra-territorial fashion. For instance, a U.S. parent requires its French affiliate to investigate a suspected violation of a U.S. law. Again, the U.S. Foreign Corrupt Practices Act (FCPA) serves as a good example. The investigation may generate documents and personal data revealing that a French employee engaged in inappropriate dealings with local government officials, only the related criminal offence arises under U.S. -- not French -- law. French privacy regulators are likely to regard such personal data to be sensitive personal data, but may not be persuaded that the U.S. law alone offers a satisfactory basis to legitimize its collection (and subsequent transfer to the U.S.). Moreover, French regulators could challenge the affiliate’s reliance on the legal claims exemption on the basis that the relevant claims -- i.e., potential FCPA violations -- relate to the U.S. parent, not its French affiliate. As discussed below, a 2005 paper released by the Working Party, supports this narrow interpretation of the legal claims exemption. In these cases, the organization needs to tread carefully and familiarize itself with the local law position.

22 With respect to its own employees, a company may be able to demonstrate that the processing is necessary to bring an action against the employee for breach of his or her employment contract, although the underlying conduct infringes other, criminal laws. Unfortunately, regulators have not provided additional guidance to assist companies looking to rely on this exemption.
Similarly, difficulties also may arise where an EU affiliate is required to collect and disclose personal data in order to assist an overseas parent respond to a foreign court order or subpoena. It is not uncommon for U.S. companies, in particular, to experience trouble when seeking to respond to disclosure demands made by U.S. tribunals or law enforcement bodies because the requisite data includes personal data held by their EU affiliates. In some Member States, it may be necessary to “localize” the disclosure demand, meaning that the EU affiliate must apply to its local court or law enforcement authority, as appropriate, for an order compelling it to disclose the data. Other Member States may be more flexible and willing to attribute any potential legal claims involving the U.S. parent to the EU affiliate because of the close corporate relationship. Besides this, consideration also may need to be given to local blocking statutes, such as France’s Law No. 80-538 of July 16, 1980, that prohibit the disclosure of documents or information of an economic, commercial, industrial, financial or technical nature to foreign public authorities. Again, this is an area where Member States appear to adopt differing approaches, with some more willing to countenance the collection and transfer of personal data in this situation than others.

3. Avoiding a Disproportionate Investigation

In Part IV, we discussed the need for companies to guard in the early stages of an investigation against engaging in fishing expeditions that result in the collection of large amounts of irrelevant data relating to employees or others, as this may offend the

23 The recent MAAF case in France demonstrates the risks arising from transferring personal data internationally where blocking statutes are present. In MAAF, a French lawyer assisting an American law firm representing a U.S. litigant in a U.S. Federal court case, sought to obtain information from the French insurer, MAAF, which was also involved in the litigation. A French court upheld a fine of 10,000 Euro imposed upon the French attorney for violating France’s 1980 blocking statute. See Cour de Cassation Chambre Criminelle [Cass. Crim.], Paris, Dec. 12, 2007, Juris-Data no. 2007-332254. Other countries, including the United Kingdom, Sweden, and the Netherlands, have enacted blocking statutes, although these tend to be more limited in scope than the French law.
proportionality principle. Once an investigation has matured to the point where the company is able to target its investigation upon a narrow set of suspects based on reliable evidence of wrongdoing, the proportionality rule represents less of an obstacle. The company still needs to keep its investigation within reasonable bounds, and not unnecessarily intrude upon a suspect’s informational privacy. And yet, the company undoubtedly will be permitted to collect and probe personal data relating to a suspect more rigorously. By way of example, in a wide-ranging inquiry into a potential wrongdoing, a company’s ability to acquire information generated long before any suspected wrongdoing occurred, in the hope that it might turn up matters of relevance, seems inconsistent with the proportionality requirement. There would be far more justification for carrying out such a review once the company has narrowed down its list of suspects and actually believes that the criminal activity extends into the past.

Despite the greater latitude afforded to companies at this stage, regulators will still expect certain safeguards to be in place. During any review of the gathered data, the company should be alert to documents that are plainly personal and marked as such. Where individuals engaged in reviewing materials encounter items, such as emails or documents, that are irrelevant to the investigation, they should be instructed to terminate their review and delete or destroy the items promptly. Unfortunately, this is not as simple an exercise as it may seem. In most cases, the individual conducting the review will need to read the materials in full before ascertaining whether it does or does not contain relevant information. By prematurely categorizing information as irrelevant, investigators risk overlooking information that could aid in the investigation. In some cases, irrelevant private material will be contained in documents that are relevant to the investigation, in which case the company should consider redacting as much personal data as possible.
4. **Responding to Access Requests**

The right individuals have to access their personal data may pose issues at the later stages of the investigation, particularly as employees or third parties begin to become nervous about the outcome of the investigation and fear they may be individually liable. These individuals may be sorely tempted to ask the company to disclose any information it has relating to them, particularly if they sense that they may need to defend themselves either in internal disciplinary hearings, before regulators or in a court room. Here, organizations ordinarily are permitted to rely on exemptions to the access rule designed to ensure the integrity of the investigative process. As noted above, Article 13 of the Directive enables Member States to waive or lighten the traditional privacy rules -- including those relating to access -- in cases where personal data are processed for the “prevention, investigation, detection, and prosecution of criminal offences, or of breaches of ethics for regulated professions” and access would place those aims in jeopardy. Whether the exemption may apply in the context of a company investigating a mere violation of corporate policy remains unsettled; in most cases it will not. Exceptionally, in the UK, a company may be relieved of its duty to provide access where it is investigating “dishonesty, malpractice or other seriously improper conduct” (including professional incompetence). However, other EU Member States appear less willing to restrict access rights on this basis alone.

5. **Transfers of Information to Third Countries**

As the above discussion on ensuring a legitimate legal basis indicates, there can be particular risks where an organization seeks to transfer personal data outside the EU to an overseas parent company or foreign authorities. The exemption to the transfer rule that permits transfers of personal data outside the EU where to do so is necessary “for the

---

establishment, exercise or defense of legal claims” may prove tempting, but can be dangerous to rely upon. Now, when the organization has gathered facts suggestive that a particular offence or wrongdoing may have taken place, there will be a tighter nexus between the personal data and potential claims. This may encourage organizations to rely on the exemption and, in the right cases, this will be appropriate. Critically, and following recent regulatory guidance released by the Article 29 Working Party, the organization may need to demonstrate that the “legal claims” relate to the EU organization, not an overseas parent, and that there is more than a mere hypothetical possibility that the claims will “one day” be brought. In WP 114, a working document entitled “On a Common Interpretation of Article 26(1) of Directive 95/46/EC, the Working Party maintained that the legal claims exemption, as well as the exemption permitting transfers on “important public interest grounds,”26 should be subject to “strict interpretation,” meaning that the legal claims in question relate not to the foreign recipient of the data, but the EU company transmitting it. According to the Article 29 Working Party, any other interpretation would “make it easy for a foreign authority to circumvent the requirement for adequate protection in the recipient country laid down in Directive 95/46.”

Relatedly, where the purpose of the data transfer is to respond to an enquiry from a foreign government or authority, the company sending the data will encounter similar difficulties, notwithstanding that the request might at first blush appear to fall within the Directive’s “public interest” exemption. Well before the Working Party embraced its “strict interpretation” approach found in WP 114, it considered and rejected in WP 66, entitled “On Transmission of Passenger Manifest Information and Other Data From Airlines to the United

26 Article 26(1)(d) provides that Member States shall permit transfers where “necessary or legally required on important public interest grounds,” as well as for “the establishment, exercise or defence of legal claims.”
States,” the use of the “public interest” exception to justify the routine transfer of personal data, so-called PNR data, relating to airline passengers by airlines entering the U.S. to U.S. immigration and law enforcement authorities. The Working Party specifically objected to a “unilateral” decision taken by a third country serving as the basis for a lawful data transfer. Accordingly, the public interest justification is not therefore likely to be available to a company that finds itself under a duty of disclosure to a foreign government, unless there is a corresponding strong public interest arising in the EU as well. In the event that neither the “legal claims” nor “public interest” exemption may be safely relied upon, organizations seeking to transfer personal data outside the EU must consider the remaining menu of compliance options canvassed above -- consent, data transfer contracts, BCRs and Safe Harbor (for U.S. transfers) -- and weigh their various advantages and disadvantages.

VI. INVESTIGATIONS & DATA PRIVACY - ISSUES UPON COMPLETION

The virtues of complying with applicable data privacy laws often becomes clearer as an investigation nears completion. Significantly, where organizations flout privacy rules when gathering information and processing personal data, they can encounter problems when trying to rely on such material in formal proceedings. Many EU Member States preclude organizations from relying on evidence seized improperly or processed in a manner contrary to data privacy norms. In the UK, for example, courts have discretion to exclude evidence “if it is necessary in order to secure a fair trial for the accused,” thus offering them the opportunity to reject information gathered improperly, perhaps because notice was withheld, a legitimate basis for processing the data was absent, or the data were unlawfully transferred outside the EU. Courts will conduct a balancing exercise to see if the prejudicial effect of submitting the evidence exceeds it probative value. Separate court applications to deal with the admissibility of evidence are only likely to detract from the real issues in the case and will
involve extra costs in the form of court and legal fees. Treading cautiously throughout the investigative process should help companies avoid these kinds of pitfalls.

Moreover, once an investigation has run its course, the guilty apprehended and the innocent exonerated, an organization still will need to be careful to avoid unwittingly violating data privacy rules. For instance, the company will have collected a large amount of material and may be unsure as to whether it should retain, delete or redact it. Three issues that often arise are the appropriate retention period for collected data; ensuring that any archived data are not used for additional purposes unconnected to the original investigation; and enabling employees access to their data.

1. **Retaining Investigative Data**

Once an investigation concludes, personal data should not be retained for longer than necessary. In the investigative context, the retention period will usually be determined by what the data reveals and whether anything significant was uncovered during the internal review, as well as the nature of any follow-up proceedings. If no incriminating material has come to light, regulators will question its retention for any significant period of time -- say, more than a few months -- unless there is an overriding legal obligation to do so. When examining the validity of compliance hotlines in WP 117, the Article 29 Working Party suggested a maximum retention period of two months if the data serves no further purpose in connection with the processing. By contrast, if the data contains information material to a subsequent legal or disciplinary proceeding, the company will be permitted to retain it for so long as proceedings are in progress and for some period of time after those conclude. This should extend up to, and perhaps slightly beyond, the point at which appeals may be lodged. During this time, the company will need to ensure appropriate security is in place to protect the data from unauthorized access, inadvertent or deliberate alteration and other unwanted disclosures.
2. **Complying with the Finality Principle**

With such a large information store in its possession, it may be tempting for the company to use the data for other, unrelated purposes once the investigation comes to a close. The “finality” or “purpose limitation” principle imposes strict limits on later uses of personal information and holds that data can only be used in accordance with the purpose for which it was obtained. What this means is that a company cannot change its mind about the use of the personal information, and any subsequent processing of the information that is unrelated to the original investigation will be in breach of the law. The Directive provides no exception, for example, that would permit a company to process the information for purposes serving other, unrelated commercial purposes. Obviously, concerns regarding unlawful secondary processing can be alleviated if the company takes steps to destroy the information as soon as practicable after proceedings have concluded.

3. **Responding to Access Requests**

It is always possible, even after legal proceedings have come to an end, that the company may receive a request from individuals whose personal data have been collected in the course of an investigation for access to their data. A recent, noticeable trend has been for persons involved or about to become involved in legal or disciplinary proceedings to assert subject access requests in an effort to acquire materials that might prove useful to their defense and to circumvent the normal timeframes for discovery. Despite this arguable abuse of subject access rights, organizations should seek to comply with such requests to the greatest extent feasible, withholding or redacting data only where there is a valid basis for doing so under local law. From a company’s perspective, once any proceedings have concluded, there should be no further need to refuse access for the purpose of preventing crime or for the purpose of effectively prosecuting the individual and so the request can normally be granted without prejudice to the employer.