



**Scott Blackmer**

Partner  
InformationLawGroup

### Compliance and Risk Management in a Multi-National World: The check list of actions and time-line considerations

When a multi-national company wants to migrate from local management of employee, client or customer personal information to a global 24/7 set of services, what are the important factors that must be considered? When the timelines are tight to reduce costs and create operational efficiencies, what risks are created in skipping critical steps in key jurisdictions? What is negotiable and what is not negotiable? What are the critical elements of the life cycle management of personal information that need to be considered up front?

Scott Blackmer speaks from years of experience in guiding multi-nationals through the maze of managing such transitions, helping Fortune 500 companies and start-ups as well navigate the complex nature of international privacy and security regulations with agility and respect.

**Nymity: Whether a company is a start-up or a Fortune 500 company wanting to verify that their global data flows are in compliance with international laws, begin a new global flow, establish a global data center or change the global flows of data, where do you do you begin with them? What are the elements of your initial discovery check list with such a company?**

**Blackmer:** First, we want to know what is triggering the company's concern with privacy-related compliance and liability. Is it a new acquisition, foreign expansion, novel outsourcing or cloud computing arrangements, a contemplated product launch or marketing campaign, a serious data security breach, questions or complaints from consumers or a trade union, inquiries from the FTC or a Canadian or European privacy commission? Or perhaps someone just got back from a conference or read an article that made her start to worry a bit! We want to make sure priority issues are addressed in the short term, while the company continues to inventory and assess all of its personal information holdings and data flows, which will typically take some time.

Second, we do suggest a "discovery" checklist to determine where the company holds personal data and where it holds the kinds of information that are most likely to get the company in trouble if the data are misused or compromised. The checklist varies somewhat according to the type of organization and its locations, but for a global retailer, service provider, or manufacturer it might include these common items:

- Identify the company's major information systems that are global or regional in scope and that contain personally identifiable data about consumers, employees, recruits, independent contractors, vendor and customer business contacts, government contacts, employees of business partners, visitors, and other individuals. Typically, these might include:
  - Enterprise resource management (ERM) systems, particularly the modules concerning human resources, customer relationship management (CRM), sales, accounts receivable, and vendor management
  - Outsourced HR, recruiting, CRM, sales, marketing, and accounting functions
  - Payment processing systems (especially any systems that capture payment card or bank account data)
  - Billing and collections systems
  - Warranty service, product returns, and customer complaint databases
  - Marketing lists or databases; behavioral marketing data
  - Website collection of personal data
  - Background checks on job candidates (references, degrees and certificates, criminal record, credit reports, security clearances, military history, driver's licenses and vehicular offenses)
  - Drug testing results for job candidates or employees

- Security, property, and IT management systems used for network provisioning and access controls, security badging, visitor's logs, and control of company-owned computers, mobile phones, vehicles, tools, and other devices and facilities
- Travel and entertainment records (corporate credit cards, corporate travel services, T&E budgets and reports)
- Equal employment opportunity (EEO) compliance reporting and diversity program records
- Security clearance records (for government contractors)
- Export control compliance records (documenting information related to nationality and residence)
- Risk management systems (records of accidents and other incidents, insurance underwriting and claims files that include named individuals, records of litigation involving customers or employees)
- Health records maintained in connection with occupational health and fitness assessments, employer-managed health insurance, company medical or emergency clinics
- Employee wellness and employee assistance program (EAP) records
- Pension and insurance benefits records (typically including information on dependents or beneficiaries as well as on current and former employees)
- Employee stock ownership programs
- Relocation assistance records (for relocated and expatriate employees; often these include information about spouses and children as well)
- Training databases
- Career development and succession planning databases
- Trade union and works council reports and correspondence
- Records of employee grievances and disciplinary actions
- Conflict of interest forms (which may contain information about family members as well as employees)
- Charitable contribution / matching gifts program records (which may tend to reveal such sensitive information as an employee's religion, ethnicity, political views, or sexual orientation).
- Identify, for each identified data collection,
  - The purposes for which the data are kept
  - How the data are collected
  - Any notices, consents, or contractual obligations associated with the data
  - The locations where the data are stored and accessed
  - Data feeds (other systems or applications that automatically access the data collection)
  - The entities or functions that have access to the data
  - How the data secured
  - How long the data are retained, and how they are disposed of at the end of their life cycle
  - Any records of complaints, investigations, security breaches, disciplinary actions, or litigation concerning a particular data collection or use.

Obviously, no one person will be able to answer all these questions, and the discovery process typically involves several different functions, departments, and affiliates. The organization would do well to designate a liaison team that represents each of these groups. In our experience, it may take months or even years before a large global enterprise really gets a comprehensive view of all of its personal data collections and data flows and establishes effective control procedures for each. This is why we try to prioritize according to the volume, sensitivity, and geographic location of the personal information.

**Nymity: Why is it now so important to understand, not only what personal or sensitive information is collected in what jurisdiction, but also how and where it is used, where it is stored, who has access to it, with whom it is shared, into and through which jurisdictions it will travel, how long it will be retained and how it will be destroyed?**

**Blackmer:** The answers to each of those questions are critical in assessing risk and ensuring compliance with applicable laws, regulations, contracts, and promises.

Legal regimes, which are often new and still changing frequently, vary in what personal data they protect and how, and in defining what activities trigger jurisdiction in a particular agency, state, or country. In the US, information that comes from a consumer reporting agency is subject to certain federal (and sometimes state) requirements concerning purpose, notice, disclosure, corrections, dispute resolution, security, retention, and ultimate disposal. The precise requirements for responding to a security breach depend on the types of information involved, the residence of the affected individuals, and sometimes the location of the data collection. Payment card data are subject to contractual security standards as well as state laws on personal information security and breach notice. Where personal data are collected, used, or stored in a jurisdiction with more comprehensive privacy or data protection laws, such as Canada, Japan, or nearly any European country, there are legal obligations and often administrative

procedures that may be unfamiliar to an American manager supervising global IT, HR, or CRM functions or negotiating a contract for business process outsourcing or cloud computing.

These issues are now getting more attention in the boardroom and the executive suite. Negative publicity surrounding a major security breach, offshore outsourcing, or a poorly conceived product or marketing decision can affect a company's public image, market share, government relations, employee morale, and even recruiting. In addition, the trend, both in the US and abroad, has been toward stricter privacy and security requirements, more substantial penalties, more intrusive consent decrees and administrative orders, and greater exposure to potential litigation damages, particularly in class actions and under statutes (such as the FCRA) that provide for statutory damages as an alternative to proving economic loss.

**Nymity: Why is it also critical to define what is personal and what is sensitive personal information by jurisdiction and globally across the company for each data subject and use/treatment?**

**Blackmer:** US managers are used to thinking in terms of specific categories of protected information, such as financial and health records, official identifiers, and information about children, students, and telephone and cable TV subscribers. These kinds of data are subject to federal laws and regulations, but the states also enact hundreds of privacy-related laws every year, so it matters to understand where the organization has customers and employees. Even where there is broad similarity – such as breach notice laws that cover SSNs, driver's license numbers, and financial account or payment card numbers – the states vary on what triggers the notice requirement, who must be notified and how, and whether a law enforcement or consumer protection agency must also be alerted. Some states add to the common list of covered information such items as health information not covered by federal law, insurance identifiers, mother's maiden name, or employee numbers, and some now require particular security measures for covered data, such as the new regulations in Massachusetts and Nevada that require a written security policy and encryption outside the firewall.

In nearly 60 other countries, virtually *any* personally identifiable information is subject to a range of legal protections. Some of those regimes (such as the national laws based on the EU Data Protection Directive) identify categories of particularly sensitive information that require additional protection, express consent, or administrative approval. Across Europe, information relating to race or ethnicity, health or sex life, political affiliation, religious or philosophical opinions, and trade union membership is subject to such additional protections, as well as national ID numbers, criminal records, security clearances, and information concerning civil judgments such as bankruptcy and child support orders. The individual countries can specify further conditions for handling what they perceive as "risky" data. Spain requires encryption of personal financial data, for example, while France and Italy require government authorization to collect biometric data or deploy geolocation applications.

Compliance is a moving target, and it very much depends on what kinds of data the organization handles, where it is collected and stored, and where the subjects of the data reside.

**Nymity: When getting ready to make a change in the above, why is it also important to know what each regulator and data subject have been told via registrations; permits; privacy notices and previously consented to in the past?**

**Blackmer:** Using data outside the scope of what was originally described and consented to is a good way to get in trouble. The FTC and state AGs have gone after many companies for selling consumer data when they said they wouldn't, and several banks have settled embarrassing lawsuits based on their sharing customer information with nonaffiliated marketers, arguably in contradiction to their express or implied promises of confidentiality.

Even where there is no contractual customer relationship, there may be liability. For example, courts have treated a posted website privacy policy as a unilateral promise on which users reasonably relied. And where a company offers opt-in or opt-out consent procedures, it must keep track of subsequent communications from the individuals changing or revoking consent.

When a company considers a new application, system, product, or policy, it should always review whether this materially changes the description of privacy practices that the company formerly published or delivered to individuals or regulators. One systematic approach is to require business or systems managers to complete a Privacy Impact Assessment (PIA) whenever they develop, acquire, or outsource a new or substantially modified information system that includes personal data. This is now a routine practice in US and Canadian federal agencies, and it would help businesses as well to identify when they are making changes that might trigger a revised privacy notice or consent form.

In Europe, companies must often register with the national data protection authority (DPA) or, in some countries such as Germany, notify their personal data processing activities to an internal data protection officer (DPO) who maintains a publicly available internal

register. Typically, no material change in personal data handling may be introduced without notifying the DPA or DPO; substantial penalties may result from changing practices without notification. We have seen cases where a company had not been registered with the DPA in a particular country because the company's activities all fell within established exemptions for routine staff administration and transaction accounting, for example, but a new marketing application or the introduction of a global ERM or intranet suddenly changed the picture and required a new or modified registration. This is particularly likely when a system is expanded to include sensitive data elements (such as health information or official identifiers) or when the data will be processed or accessed outside Europe.

**Nymity: What about the various types of labor unions and works councils in the EU and other jurisdictions? What kinds of powers do these entities possess? What are the risks if they are overlooked?**

**Blackmer:** In the US, collective bargaining agreements traditionally did not address workplace privacy issues, apart from the confidentiality of grievance procedures. Some now include provisions on drug testing, computer and communications monitoring, video surveillance in restrooms and changing rooms, and genetic testing – all areas that have received recent publicity. Similar issues have arisen in collective bargaining in Canada and Australia.

In Europe, national laws (many of them based on an EU directive) typically provide for a form of elected employee representation generically known as “works councils,” in addition to any national or employer-specific union contracts that apply. Works councils must be consulted on issues that substantially affect employees, in sufficient time for them to contribute comments before a decision is implemented. The planned introduction of outsourcing or global ERM applications often results in a lengthy discussion between management and the relevant works councils, sometimes resulting in changes to meet employee concerns. In some cases, a works council has asked the data protection authority for an opinion on particularly sensitive issues.

On some matters, particularly in Germany and Austria, works councils have co-decision powers as well as a right of consultation. This means that the employer would have to seek arbitration before a labor tribunal before it could implement a decision to which the works council did not accede. In some cases, a decision to close a local data center in favor of outsourcing or global consolidation could trigger the co-decision procedure. Importantly, German labor tribunals have ruled that decisions about deploying or modifying automated data processing systems containing employee data are subject to the co-decision powers of works councils. Consequently, in addition to an explanation from management concerning the risks and benefits related to such a decision, German works councils will generally require an opinion from the internal data protection officer, who is entitled to consult with the state data protection authority if the DPO deems that useful, and then produce a written opinion concerning the plan. The works council may object or ask for changes in the plan based on privacy concerns, and ultimately the issue could be submitted to either the data protection authority or labor tribunal. Thus, the process of consultation and approval may take anything from a few days or weeks to several months. Many corporate plans for outsourcing, consolidation, or global access to HR databases have been held hostage to the concerns of German works councils, and in some cases the programs were simply not implemented in Germany as a result.

**Nymity: What about the time factors? What are the important privacy actions that must be taken into account that affect the overall implementation timeline? Why is it imperative that these actions and the associated time considerations be taken seriously? Please provide some examples where the timeframe might be long, but critical to the overall success of the information initiative.**

**Blackmer:** The organization should include a privacy compliance and risk management review in the process of designing, approving, and deploying any new or substantially modified information system that involves customer or employee data. I mentioned the Privacy Impact Assessment above as one way to standardize that review and raise the awareness of project managers early in the process. The privacy officer or liaison team can then offer advice on how to avoid or minimize risks. One client, for example, targets a couple dozen sensitive data elements (such as SSN and family information) and requires managers to explain why they need to include any of those elements in the system and how they will control access to those elements. It is generally cheaper and easier to design systems with these factors in mind than to retrofit them later with privacy controls.

If a proposal involves transferring European or Canadian data (or data from another jurisdiction with strict privacy laws) to the US or another jurisdiction with dissimilar legal protections, the organization needs to take steps to comply with requirements in each of the data “exporting” countries, to avoid creating liability for the foreign affiliate or business partner or inviting a disruptive “stop processing” order from the foreign authorities or courts. Data transfers to the US from the EU/EEA countries and Switzerland typically must be based on informed consent or protected by EU-approved standard contract clauses, the EU or Swiss Safe Harbor Frameworks, or approved “binding corporate rules” (BCRs) – otherwise, the exporting company may be fined, sued, or ordered to suspend data transfers.

Producing a data transfer agreement with EU standard contract clauses requires a little time, since it must include an annex describing the transfers and it must be signed by representatives of each of the legal entities involved. More importantly, the US headquarters company (or Indian outsourcing vendor) must be prepared to implement protections that are essentially similar to the rules that would apply in the data subjects' home country.

Safe Harbor certification similarly can be effected in minutes online at a US Department of Commerce website, but implementation, training, and annual assessment take some time. Clients usually require several months of review, policy documentation, and training before an officer is willing to certify to the Department of Commerce that the company handles European personal data consistently with the Safe Harbor Privacy Principles.

Safe Harbor participation avoids a lengthy review and approval process in the affected European countries, but the company's data protection notices and registrations still must be updated to reflect data transfers under the Safe Harbor program. Where the organization relies on standard contract clauses instead, many European countries require prior authorization, which can take two to four months (or longer if there are questions). BCRs, the newer and less tested procedure for legalizing cross-border data flows from Europe, typically require more than a year to finalize and gain approval from the relevant authorities.

Thus, a project involving the transfer of European personal data to the US, India, or other jurisdictions that are not subject to an EU "adequacy" decision requires some advance compliance planning. The preferred legal basis must be determined and then reflected in notices to the individuals, appropriate contracts, and notifications to the authorities, which in some cases require prior authorization before the data flows can begin. Safe Harbor is the quickest route on the European side, but in all cases the company has to concern itself with appropriate internal implementation and training.

The prior discussion about German works councils explains why companies may need a longer lead time before launching an information system that includes German employee data, especially if it includes sensitive data or involves storing or accessing the data overseas. But works councils in other countries may also need to be consulted in advance, even if they do not have co-decision powers over the decision.

**Nymity: What about the variations in the law? Must all of these different local regulations be followed? Please provide examples where the law must be followed; where it might be acceptable to perhaps not follow all of the laws to the letter, if there are such examples.**

**Blackmer:** I've given examples of local variations in the law, both within the US and internationally, in responding to the earlier questions. As a lawyer, I can't advise anyone to ignore an applicable law, although it is clear that some violations have graver consequences than others. And in some cases, particularly under the broad-brush European data protection statutes, it is really unclear what is the precise scope and application of a requirement or exemption, so a company must make its own determination or, in critical instances, seek an opinion from the relevant authorities. Clients are often daunted by the task of matching ever-changing technology and applications against proliferating and evolving legal standards, but it makes sense to prioritize compliance efforts according to the volume and sensitivity of the data involved and to establish internal procedures such as the PIA to get a grip on the issues going forward.

As for the consequences of noncompliance, there is more litigation in the US around consumer reports and violations of communications privacy, because statutory damages are available in those areas even if economic loss is hard to prove. Those statutory amounts can be cumulated in a class action or a complaint filed by one or more state attorneys general. The FTC and some states have aggressively pursued companies that have violated their own privacy terms or that have been negligent in protecting personal information such as SSNs and payment card details that are particularly at risk for identity theft. For GLBA and HIPAA violations, which do not directly give rise to private lawsuits, the concern is more that the regulators will impose fines, oblige the company to establish a fund to compensate injured individuals, or require the company to make certain operational changes and in some cases submit to independent privacy and security audits. The security and breach notice laws in the states have resulted in some litigation, but their principal effect is in publicizing security failures and imposing prevention and response costs. The latter include the costs of notice and remedial measures, such as providing credit monitoring services and replacement cards or accounts, that are undertaken for customer or employee relations purposes rather than as a legal obligation. Companies also have to take into account the public relations and market impacts of controversial privacy practices or of large or repeated security breaches. And in some areas, such as processing and storing payment card data, companies are subject to contractual obligations that might result in their losing access to a business partner or payment network if they are deemed careless in handling the data.

Outside the US, individuals very seldom sue companies over privacy violations, even where that is theoretically possible. Unlike the US, there is typically no provision for class actions; the complainant in some countries must pay the defendant's legal and court fees if he does not prevail; there is no broad discovery of the defendant's internal documents and communications; lawyers are not allowed to take cases on a contingency fee basis; and punitive or exemplary damages are seldom available. Moreover, in Europe, Canada, and several other countries, there is a ready alternative: it costs the complainant nothing to approach the national or provincial privacy commission or data protection authority. Those authorities have investigative powers and, in many countries, the power to issue orders and fines as well as the discretion to publicize egregious cases or submit them to the justice ministry for prosecution. In most cases the authorities deal discreetly with the company to improve its practices; few companies are publicly denounced and fined. Some of the most common issues that result in strong administrative action are handling sensitive data without authorization, failing to implement marketing opt-outs, covertly collecting and sharing information, and engaging in practices inconsistent with the organization's announced privacy policies and data protection registrations. More recently, European authorities have also expressed greater concern about large-scale security breaches involving personal information.

**Nymity: What are some of the implementation considerations that need to be factored into the implementation plan or task list? What can slow the process down? What can help speed the process up?**

**Blackmer:** In addition to some of the international and cross-border issues discussed earlier that may take some time -- such as consulting works councils, making filings with European data protection authorities early enough to avoid launch delays, and putting contracts, Safe Harbor, or other transborder compliance vehicles in place beforehand, there are some steps that will generally facilitate privacy compliance and risk management for existing systems and for projects involving new data applications:

- Establish a multi-departmental privacy team with a designated lead person who reports directly to senior management. Include internal or external subject matter experts in the areas of greatest need.
- Document and update information security, privacy, and data retention policies and procedures.
- Chart the company's data collections and data flows, especially tracking the sensitive categories of data.
- Substitute employee or customer numbers for SSNs and other official identifiers wherever possible.
- Consider deploying automated solutions, such as software that detects SSNs and payment card numbers in databases and communications, and software that identifies company web pages that collect data from users.
- Tag or segregate data that is subject to specific legal or contractual requirements, such as HIPAA data, payment card details, reports from credit bureaus, and HR and customer data from Europe.
- Deploy online training for staff members and contractors who handle personal data.
- Implement a Privacy Impact Assessment procedure to bring privacy issues to light early in IT, HR, and marketing projects.
- Use industry and professional associations, specialized information services, and expert advisors as needed to keep up with privacy developments in the relevant industry and jurisdictions.

**Nymity: In a multi-national company that does business in 150+ countries what are some techniques for simplifying implementation processes?**

**Blackmer:**

- Establish high-level privacy principles, expressed in plain language, that apply throughout the organization, supplemented by more detailed and specialized privacy policies for data covered by specific regimes, such as HIPAA, PCI DSS, or Safe Harbor, which ideally should be tagged or segregated for ease of training and implementation.
- Bridge the gap between the organization's privacy and security policies. For example, if the organization uses a security classification scheme ("confidential," "highly confidential," "proprietary," etc.), indicate how personal data are classified, and apply the more restrictive security practices to the more sensitive kinds of personal data. Some organizations simplify by treating all personally identifiable data as the equivalent of company proprietary data, and a list of sensitive data elements as highly confidential data.
- To collect information online from consumers, employees, or job candidates, consider standardizing on a single website privacy statement and form that satisfies all the relevant requirements (typically, this means referring to the California website privacy law and the notice and opt-out requirements of laws based on the EU Data Protection Directive).
- Some companies standardize on privacy policies generally that satisfy the strictest regimes or commonest standards in the states and countries in which they operate, even though these exceed requirements elsewhere. In the context of breach notice in the US, for example, this means providing the same notice and remedies nationwide, regardless of the "harm" threshold that applies in some states. In practice, this may be easier to implement and explain to the public than a policy of providing notice only in the states where it is absolutely required. Internationally, the EU Data Protection Directive, the Safe Harbor Privacy Principles, the OECD Privacy Guidelines, and the APEC Privacy Framework have each been used as the basis for a company-wide approach to privacy, even though the source document goes beyond the legal requirements in

some of the relevant jurisdictions. There will inevitably be some peculiar local requirements that have to be addressed as well, but a strong, consistent, overall approach to privacy is likely to raise awareness internally and avoid problems with individuals and regulators.

- For data flows from Europe to the US (and onward from the US), the Safe Harbor Framework is simpler and more standard than a multiplicity of contracts with EU-approved standard contract clauses. However, the latter may still be required for data flows directly from Europe to countries other than the United States. A few large global companies have adopted binding corporate rules (BCRs), approved by the relevant European data protection authorities, that cover all data flows within the corporate group; this solution takes more time but may be worth the investment for a very large and complex organization.
- Security measures required for privacy protection are usually not spelled out in laws and regulations, which typically refer only to “reasonable and appropriate” safeguards reflecting the sensitivity of the information and the likely risks of loss, theft, or hacking. Rather than make this analysis country by country and sector by sector, many multinationals establish global policies and procedures based on widely accepted standards for information security management systems, such as ISO 27001 / 27002, the PCI DSS standard for payment card data, relevant NIST guidelines, or the FTC’s GLBA Security Rule. Several jurisdictions require written security policies for at least some categories of personal information, and it is convenient to be able to refer to a single, company-wide document that addresses security for personal data.

**Nymity: In a smaller start-up multi-national company what are some of the standard setup processes that are essential for such a company, regardless of size?**

**Blackmer:** A start-up can be instantly multinational, at least in its customer base, thanks to the Internet. The advice above for large multinationals applies as well, and in some instances it’s easier for the start-up to implement, since it does not have to troll through established databases, legacy applications, and hundreds of web pages to find personal information and conflicting privacy statements. The start-up can either restrict customers to jurisdictions where it is confident of compliance, or it can standardize on practices that satisfy the strictest regimes.

**Nymity: In closing, it used to be local, now it is global with services that are 24/7. What have we not asked, that would be meaningful for our readers to know about?**

**Blackmer:** Most privacy-related issues can be defused if the company informs itself concerning relevant legal and contractual obligations, publishes a readable privacy policy, available online 24/7 as well as on documents collecting personal information, lives up to its announced policies, and establishes a point of contact for privacy inquiries and complaints, preferably accessible by phone or email. The contact point can be used not only to satisfy individual concerns but also to provide feedback on what a company’s customers and employees find confusing or objectionable.

Security breaches can scuttle a company’s reputation despite the best policies and intentions. There are really only two alternatives: don’t collect and store personal information (especially the more heavily regulated categories), or keep up to date with security risks and countermeasures to protect the confidentiality of whatever personal information the organization must maintain. Refer wherever possible to procedural and substantive security standards, which will tend to avoid breaches and furnish a legal defense of reasonable care. Exercise due diligence in outsourcing, and monitor outsourced transactions, processing, and storage. In the eyes of the law and of the public, you cannot really outsource ultimate responsibility for the information you collect and use.