Conducting a Privacy Audit

By Michael L. Whitener

A glance at the headlines reveals that data privacy breaches are increasingly common, and the consequences to corporations — in terms of reputational damage, potential liability and costs to remedy — are increasingly dire. To avoid those consequences, any corporate entity that collects, uses or transfers personal information must take steps to ensure it is complying with legal requirements for maintaining data privacy and — equally important — living up to the trust of its employees, customers, partners and suppliers. A privacy audit provides a means of benchmarking corporate privacy practices against what the law requires and what industry best practices demand.

So what exactly does a privacy audit entail? As explained below, it need not be a daunting or expensive undertaking. With the proper tools, support from corporate management, a motivated audit team and a few guidelines, a privacy audit can be conducted using primarily internal resources and with little or no business disruption. If properly carried out, a privacy audit will result in a clear understanding of an organization’s personal data flows and a comprehensive information security/privacy program that will protect personal data from unlawful collection, handling and disclosure.

**Types of Privacy Audits**

Broadly speaking, there are two types of privacy audits: an “adequacy” audit and a “compliance” audit.

**Adequacy Audit**

An adequacy audit is aimed at: 1) determining whether an organization’s data privacy policies are adequate to address the requirements of all applicable data protection laws and regulations, both domestic and international; and 2) making sure they apply to all data processing that an organization actually conducts. This type of audit involves not only a review of all company policies, procedures, codes of practice and guidelines that affect the handling of personal data, both within the company and in dealing with third parties such as vendors and suppliers, but also requires an understanding and mapping of data flows across the enterprise.

An adequacy audit may well reveal serious gaps in an organization’s data privacy policies, given the types of personal data being handled and the ways it is being stored, transferred and otherwise processed. In that case, while an organization could proceed right away with conducting a compliance audit, the better practice, in my view, is to first remedy the policies and procedures found wanting before continuing on to the compliance audit.

Why? Because the purpose of a compliance audit is to determine whether a company is hitting its targets in terms of the objectives established by its privacy program. If those targets are nonexistent, or poorly placed, it will be a false victory to declare that they have been achieved.

**Compliance Audit**

The compliance audit sets a higher hurdle than the adequacy audit: to determine whether an organization is actually abiding by the policies and procedures identified during (and perhaps improved as a result of) the adequacy audit. It requires an investigation of how personal data is handled in practice within the various business units, across departments, and when dealing with third parties.

A comprehensive compliance audit should also examine such factors as whether the organization offers data privacy compliance training, how data privacy policies are disseminated to employees, and how complaints of policy violations are handled. The depth of the compliance audit will depend upon the perceived risks to the enterprise of legal violations and data breaches.

**Tools for a Privacy Audit**

There are two essential tools in a privacy audit toolkit: 1) questionnaires and follow-up interviews, aimed at mapping data flows and processing; and 2) a data privacy table or matrix that allows the tabulation of the results of the audit.

**Questionnaires and Interviews**

For both the adequacy and the compliance audit, drafting of a questionnaire to be completed by the various business units that handle personal data is a critical step. The questionnaire should seek answers to questions such as the following: 1) **What are the purposes for which personal data is being collected?** For example: customer administration, employee administration, advertising and marketing. 2) **What individual’s personal data is being processed?** For example: customers, employees, suppliers,
consultants. 3) **What types of personal data is being collected?** For example: names, addresses, telephone numbers, occupational details, social security numbers or ID numbers, and financial information. Particular attention should be paid to any personal data that might be considered “sensitive.” In the EU, sensitive data includes that pertaining to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health matters and sexual orientation. 4) **How is personal data collected?** For example: hard copy form, online, by telephone or from third parties. 5) **Is the consent of the individual obtained?** If so, by what means, and at what point in the collection process? 6) **How relevant is the personal data for the purposes collected?** Would anonymized personal data be equally relevant? 7) **What steps are taken to ensure that the accuracy of personal data is maintained during the period of retention?** 8) **How long is personal data retained?** Is this retention period really necessary — e.g., legally mandated? Or is personal data being held for longer than required to meet legal obligations or for reasonable business purposes? 9) **Where and how is personal data stored?** 10) **What technical and organizational security measures are taken to protect personal data against unauthorized access, damage or erasure?** For example: encryption, use of secure passwords, contingency plans and training. 11) **Is the personal data disclosed to any third parties?** If so, for what purposes? What additional security measures are taken to protect disclosed personal data from unauthorized access, damage or disclosure — e.g., written contracts with third parties that impose specific data security and privacy obligations? 12) **Is personal data transferred outside the country in which it is collected?** If so, what consents are obtained and what additional security measures are taken? 13) **Are there procedures in place to allow individuals to access and control use of their personal data?** For example: opportunities to correct inaccurate personal data, delete irrelevant personal data, and prevent personal data from being used for marketing purposes. 14) **How is personal data that is no longer required disposed of?** Does the method of disposal/destruction ensure that the personal data cannot be accessed again? Answers to the questionnaire should be collected from each of the business units that may handle personal data — typically including human resources, information technology, marketing and customer sales/support. Each of the department heads should be tasked with responsibility for ensuring that the questionnaire is completed fully and accurately.

Inevitably, responses to the questionnaire will raise additional questions, which is where the follow-up interview comes in. Personal interviews with executives and employees responsible for handling personal data within an organization allow for a deeper dive into the “whys” and “hows” of personal data processing. For example, the questionnaire may reveal that the HR department is retaining employee information for years after an employee has left the company, but not the rationale for such retention. The rationale can be explored during a follow-up interview.

The importance of the questionnaire and follow-up interview in determining compliance with data privacy policies should be obvious, but the responses are equally important in determining the adequacy of the policies themselves. Too many companies put privacy policies in place with only a dim understanding of how applicable they are to actual enterprise data flows. The questionnaire/intererview responses should be geared toward making sure that there is alignment between policies and actual personal data collection and handling.

**Privacy Adequacy and Compliance Matrix**

The other essential privacy audit tool is a matrix that organizes the results of the audit questionnaire as well as the review of an organization’s privacy policies and procedures. The format for this matrix that I have found most useful is a table with the following headings:

- Privacy principles, which states the specific privacy principle (likely required by law) that the organization is seeking to achieve.
- Description, which describes the privacy principle in some detail.
- Documented policy, which references the organization policy (with citation to a specific section) that is intended to satisfy the privacy principle. If no documented policy exists, that should be noted.
- Compliance with principle, which describes whether the organization is actually complying with the principle and the related organization policy.
- Gaps/weaknesses, where any failures of the organization to abide by the privacy principle and related documented policy can be noted.
- Notes, to indicate any follow-up tasks.

In deciding what privacy principles should be achieved, an organization need not start from scratch. There are a number of templates that can be reviewed and borrowed from. Personally, I have found the privacy risk assessment tool developed jointly by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants, based upon Generally Accepted Privacy Principles, to be the especially helpful for this purpose. In the EU, some national data protection authorities have issued their own auditing guidelines. For instance, the Netherlands has published a Privacy Audit Framework to guide the auditing process.

While an audit report should also contain a narrative of audit results and conclusions, the adequacy/compliance matrix provides a convenient method for compiling the results of the privacy audit in easily understandable form and for ready reference. Equally important, the matrix allows for ready apples-to-apples benchmarking of an organization’s progress in satisfying relevant data privacy requirements from year to year.

**PROCEDURES**

**Assembling an Audit Team**

A threshold question when preparing for a privacy audit is whether the audit will be conducted internally, or by an outside audit team, or using some mixture of internal and external resources. There are several
advantages to conducting a privacy audit using existing corporate resources, including the internal audit team if there is one: 1) It is less costly; 2) Employees will have a better understanding of the corporate organization and activities than outsiders; and 3) The learning process of conducting an internal privacy audit will prove useful for corporate data privacy awareness and post-audit monitoring purposes.

A few disadvantages to using an internal audit team should be noted, however: 1) They are potentially less objective and rigorous than an independent, third-party audit team; 2) The audit results may carry less weight externally — e.g., with legal authorities if a data breach does occur; and 3) An internal audit team, unlike a “hired guns” team, will not readily be able to benchmark the audit results against the results of auditing other similarly placed organizations.

In my opinion, the solution that best combines audit depth and comprehensiveness with cost efficiency is to use an in-house audit team (including representatives from Legal, Finance, HR, IT and Marketing) under the guidance of an outside privacy audit professional. That way, an organization reaps the advantages of internal institutional knowledge along with the objectivity and experience of someone with privacy audit experience under his/her belt.

Setting the Tone at the Top

Once it is determined how the audit team will be comprised, and an audit start date is agreed, it is important to consider the “messaging” of the audit undertaking. As with all corporate legal compliance initiatives, the “tone at the top” is critical.

One tried-and-true strategy is for the CEO to send out a memorandum describing why a privacy audit is being conducted, who will be leading the effort, and what participation will be required from the various business units. A memorandum with the CEO’s imprimatur will help overcome any reluctance of staff to set aside their usual duties to support the auditing effort. If appropriate, the memorandum should note that the board of directors is fully behind the audit.

The Aftermath

Once the privacy audit is completed, an audit report should be prepared. The audit report will include the privacy adequacy and compliance matrix discussed earlier, which itself will incorporate the results of the questionnaire and follow-up interviews as well as the review of the organization’s policies and procedures. The audit report should also include a narrative that addresses such factors as: 1) the methodology of the privacy audit; 2) who was responsible for the audit; 3) conclusions, including any identified privacy gaps and weaknesses; and 4) recommended remedial actions, including employee training.

For purposes ofremedying any gaps in existing organization policies and procedures, one option, of course, would be to create a new information security/data privacy program from whole cloth. There may be merit to such an approach, depending upon how antiquated existing policies are and how much the organization’s data processing activities have changed since the policies were put in place.

However, the organization may also find that they already have many of the elements necessary for a robust, up-to-date data protection program — an acceptable use policy here, an online privacy policy there — and can knit these disparate pieces together into a comprehensive program that only requires filling in a few gaps. Related policies can be grouped under an umbrella policy that functions as a data privacy mission statement. What is crucial is that the audit report be the basis for action, whether that action is drafting or revising privacy policies or taking steps to ensure compliance with policies already in place.

Conclusion

In the data privacy sphere, the one constant is change. Privacy issues are getting increasingly high priority on political and social agendas as the ease with which personal data can be collected, stored, marketed and transferred globally has expanded and the term “Big Data” has entered the vocabulary. One consequence has been more stringent data protection requirements and more draconian penalties for violations — witness the EU’s proposal to impose penalties for violating the EU Data Protection Directive of up to 2% of a company’s global annual turnover.

In this environment, the protection of personal data is paramount. Conducting a data privacy audit allows a real-time assessment of how well an organization is living up to its data protection legal obligations as well as the expectations of its customers, employees and others. Such an audit simply makes good business sense and need not drain corporate resources, financial or otherwise.