Kodak's approach to global privacy compliance

At PL&B's annual International conference in July, **Dale Skivington** and **Helen Isaacs** explained how Kodak implemented its global privacy compliance regime. Report by **Alan Pedersen**.

One of the key elements in developing a successful privacy compliance programme, said Dale Skivington, Chief Privacy Officer (CPO) for the Eastman Kodak Company, is support from the top. One of the first tasks following her appointment as the organisation's first CPO was to liaise with key decision makers with the view to revising its existing practices and developing a robust corporate policy on privacy protection. "When I first took this job, Kodak had a policy on management of confidential information," said Skivington. "We essentially decided to change that policy and create one on just personal data."

Initiating meetings with Kodak's president, general counsel, chief marketing and financial officers, Skivington obtained the necessary commitment and backing to start implementing Kodak's privacy programme. This led to the creation of a corporate privacy council, made up of representatives from departments including legal, marketing, HR, and government affairs.

Reporting to the council was a global privacy task force, set up with the aim of developing and implementing Kodak's data protection policy. Over time, Kodak has developed an impressive privacy compliance framework outlining the role that privacy plays throughout the organisation (see box on p.23).

The framework now covers a range of areas, handled by teams such as the marketing privacy council, an HR/medical data compliance team, a training unit, and regional privacy teams handling specific legislation such as the EU Data Protection Directive.

In building a culture of privacy across the organisation, Skivington explained there were two approaches she could have taken. "One was to build an organisation of people who reported to me, who were privacy professionals, to implement a programme at Kodak," she said. "The other approach was to say: 'everybody plays a role with respect to privacy. Anybody who touches data has a role.'" Through this approach, said Skivington, the marketing division takes ownership of any privacy issues surrounding marketing, and similarly, HR takes control of staff privacy compliance.

Over time, Kodak has developed an impressive privacy compliance framework outlining the role that privacy plays throughout the organisation.

Assessing internal compliance standards

Once Kodak had decided upon its policy approach, it began an assessment of its internal control standards. "I believe how you manage data, in terms of how it is actually handled within your company and by third parties," said Skivington, "is probably the most important thing a CPO does after setting those policy decisions."

One of the first projects was to look at the emerging Internet side of the business. An online privacy council was established to develop a coordinated approach to privacy compliance across the various business units within Kodak. Co-chaired by the CPO and the chief marketing officer, and made up of representatives from each business unit, the council meets on a monthly basis to examine issues such as online privacy policies and marketing preferences systems. The council has also appointed a compliance manager to ensure that new initiatives and projects are fully assessed and audited against the company's privacy policy.

Agreeing a common approach to compliance may sound simple in theory, but Skivington said such a process is no easy task, especially in organisations made up of diverse business units. Kodak is not just a consumer-focussed organisation, but has business-business units and areas dealing with resellers.

Despite the complexities, the online privacy council has had its successes, one of the first being the creation of a single combined privacy policy for e-customers. "People couldn't believe that we got all our business units to agree to one set of terms and conditions with respect to privacy on the Internet," said Skivington. "But essentially again you go back to the brand issue – what is right for the customer, what the customer wants."

The council also came up with a coordinated approach to customers' marketing preferences. Business units brought their resources together, linking up previously separated databases to develop one single database for handling marketing preferences. The project was so successful, said Skivington, that Kodak is now looking at extending this concept to offline data collection.

Privacy in Europe

Despite developing a global approach to privacy compliance, there was also a need to look at compliance on a regional level, especially because of the EU Data Protection Directive. Kodak set up a number of regional privacy teams covering Latin America, Asia, Canada, and Europe, Middle East & Africa (EMEA). Helen Isaacs, legal business manager for Kodak UK was handed the EMEA region, acting as a coordinator between the business units within the EMEA region and Kodak's CPO.

European works councils

A major issue for the EMEA privacy team has been liaising with the various works councils across Europe. "Data privacy has been their top issue every meeting since we formed our European Works Council in 2000," said Skivington, adding that its members have repeatedly asked for privacy experts to attend meetings.

Isaacs outlined developments with the works councils over Kodak's plans to implement a global HR system. "One of the surprises we got was in terms of the very high level of interest from the works councils, particularly in Germany," she said. "They've been very concerned in terms of what we are doing with the global HR database, what data we are putting onto it, what levels of manager might be accessing this database, and in which countries."

> "One of the surprises we got was in terms of the very high level of interest from the works councils…They've been very concerned in terms of what we are doing with the global HR database"
>
> **- Helen Isaacs, legal business manager for Kodak UK**

The approach from the EMEA angle, said Isaacs, was to develop a network of localised data protection officers that "we use both for sharing information, but also getting them to input on what Kodak is doing on a global basis." This, she said, helps Kodak to achieve a consistent approach to privacy across the organisation.

Isaacs explained that one of her initial tasks was to adapt Kodak's corporate privacy policy to take EU legislation into account. "While we were following the corporate policy, she said, "we needed to go one step further in terms of the instructions we were giving to the countries in EMEA…we felt there was a need to take our corporate policy on the privacy of personal data, and to regionalise it." As a result, a set of regional implementation guidelines was developed to reflect the legal variations across Europe.

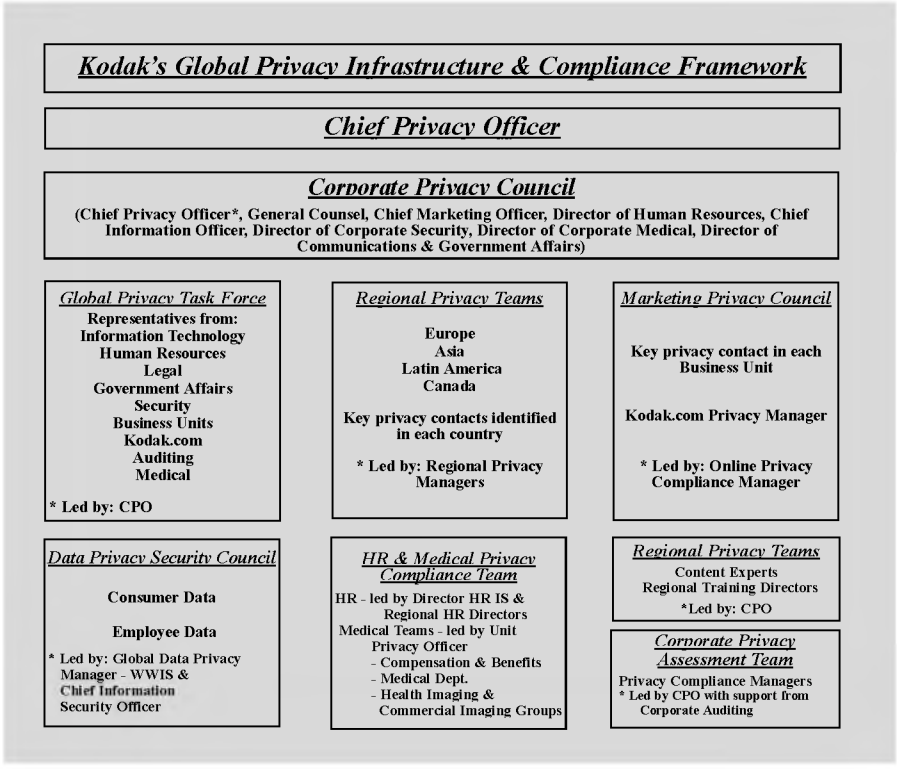
This approach also meant creating country-specific versions of Kodak's online privacy policy. "We've taken Kodak's policy and translated and localised it for 18 countries" Additionally, said Isaacs, "we now have a network of contacts for queries, by line of business and by country, and we are developing that further as countries come into the EU."

Kodak decided to take a proactive approach to liaising with the works councils, providing them with information on its implementation strategy for the HR system, how cross-border transfers would be handled, what the access controls would be, and so on. Demonstrating that Kodak is taking the issue seriously, said Isaacs, is the "best way of trying to instill confidence into them that we are doing the right thing."

Skivington said that an upfront approach with proactive consultation helps avoid future barriers to progress. "I know from some of my peers who didn't take this step," she said, "and went ahead and purchased the [HR] software and tried to implement it without having that dialogue - they were stopped in their tracks by their works councils."

Applying security controls

Kodak's previous system for securing personal data, said Skivington, would rely on labeling records containing personal data in a certain way, and then applying specific controls to that record. A highly confidential record would, therefore, contain stricter controls than less sensitive information. However, Skivington saw weaknesses in this approach. "If the label doesn't go onto that document, it flows to the bottom of the least rigid control." So if not properly labeled, documents or



records containing sensitive information would, therefore, be at greater risk than they should be.

To remedy the problem, said Skivington, Kodak engaged in a year-long activity, setting up a global team to look at every data element that needed reviewing – for example, credit card details, medical data, and any information that could be considered sensitive from any person's or any country's perspective.

Once the data flows across the organisation had been identified, they then figured out exactly what set of controls should be applied. After analysing the various security standards that existed (such as the ISO 7799 and HIPAA security standards), they developed a standard for each data element and then benchmarked them with other companies in Europe and the US. The result was a set of best practices per data element. "If you look at medical information," said Skivington, "it takes you right through from the creation of the document, to the destruction of the document, to transmittal, to storage."

In addition to security controls, Kodak developed a privacy self-assessment tool which checks the compliance standards for each new data collection system before letting the application go live.

THIRD PARTY PROCESSORS

Skivington explained that Kodak developed a two-tier approach to third party processors. Firstly, they would look at the risks of a particular outsourcing operation, examining a number of criteria such as the amount and sensitivity of the data involved. Then, depending upon a high/medium/low assessment of the risks, Kodak would then either do a full-blown assessment of the processor involved or, at the other end of the scale, send out a questionnaire based upon its internal control standards. In cases where the risks are extremely high, said Skivington, outside inspections could be carried out, either by Kodak itself or a third party assessor.

Actually identifying these processors, said Skivington, is "one of the toughest things to do." Nonetheless, Kodak scoured its systems for third party processor contracts and then examined what they said about privacy. She discovered that there were weaknesses in the contracts. Although there were "confidentiality of communications" clauses, there was a need to develop robust privacy and security provisions into all the contracts. "I worked with my global team to develop a set of terms and conditions for privacy and security," she said, explaining that Kodak then went back and renegotiated its contracts with third party vendors.

> "I believe how you manage data, in terms of how it is actually handled within your company and by third parties is probably the most important thing a CPO does after setting those policy decisions."
>
> **- Dale Skivington, Chief Privacy Officer, Kodak**

AUDITING COMPLIANCE

Skivington explained that a compliance auditing team was set up, which comprises of data protection officers from each business unit and geographical region. The organisation undergoes annual audits, with every 'record owner' (eg. every database has a record owner) using an assessment tool to monitor areas such as access controls, record retention, third party access to information, and contract language.

In addition to annual audits, Kodak also carries out spot checking and third party assessments on some of the more sensitive areas of the business.

Isaacs said that these audits have received a great deal of attention from the business areas within the organisation. She explained that this was less to do with the regulatory threat of enforcement action, but rather because the results are reported back to the chief marketing officer. The threat of internal action, it seems, is a more persuasive driver for privacy compliance than outside forces. "It's a very good way of focussing attention and getting everything achieved," said Isaacs.

TRAINING

Procedures and rules are one thing, but as Skivington pointed out, educating staff about privacy is key. "You can't do privacy without having a good training strategy," she said, "because some of this stuff just doesn't come naturally." The first step was to actually find out what level of knowledge staff had, so assessments were carried out on how many people had read the organisation's internal control standards. The resulting evidence showed a knowledge gap that needed to be addressed. As a result, Kodak is now in the process of rolling out a training programme for 70,000 employees handling HR or customer data. Special training modules, specifically tailored to meet the needs of staff in areas such as marketing, HR, and IT services, will also be provided, in addition to advanced training for staff who handle medical information.

Additionally, said Isaacs, there is specific data protection training for staff outside the EU handling personal data from European customers or staff.

USING BRAND AS AN INTERNAL PRIVACY DRIVER

Buy-in on privacy from across the organisation has played a major role in developing a culture of privacy compliance within Kodak, said Skivington. "There isn't a single manager at Kodak that doesn't understand that our most important assets are our people, our products and our brand…Every single employee at Kodak understands the importance of our brand. Therefore, privacy becomes very easy."

It is because of this recognition of the role that privacy plays in the status of the corporate brand, said Skivington, that friction with business units in the organisation is avoided. "Because we believe privacy is so tied to the brand, we hold everyone accountable, said Skivington. "We have literally hundreds of people who have some responsibility for the privacy regime at Kodak, and they're held to account through our assessment processes."