How IBM manages marketing compliance

Dr Armgard von Reden, IBM's chief privacy officer for Europe, Middle East and Africa, talks to *PL&B International* about how IBM has developed a global standard for privacy-compliant marketing.

IBM is one of those truly global giants. Currently ranked in the top 10 of the US Fortune 500 and with a presence in just about every country you could imagine, IBM is a leading player in the computer hardware, software and IT services sectors. Described by *Business Week* in 2002 as having the third most valuable worldwide brand, IBM has established an enviable status it will be keen to protect. Which shows why the organisation has put a great deal of effort into establishing responsible marketing practices and strong data protection standards.

When it comes to marketing compliance, the European Union has arguably the most stringent data protection regulations, with a lack of conformity between national laws that can hinder multinationals' efforts to operate a standard system for its business processes. So how does IBM ensure its marketing operations meet the legal requirements?

Compliance strategy

Armgard von Reden explains that IBM's marketing strategies will vary according to the business unit involved or the product and service being advertised. While some campaigns are carried out nationally, others are conducted on a pan-European or global level. Because there is a significant number of cross-border campaigns, von Reden explains that IBM decided to adopt a global privacy standard that enables it to be compliant across all jurisdictions.

Although most European data protection laws impose fewer restrictions on marketing to business contacts, IBM has chosen to standardise the marketing choices it offers, whether it is for customers in large enterprises, small businesses or private users. It does, however, vary its approach according to which channel is used to deliver marketing material. While customers are offered the opportunity to opt-out from being contacted by direct mail, (telephone contact is used for IBM customers only), an opt-in choice is given for e-mail marketing. The decision to adopt a higher standard of consent for contact by e-mail, explains von Reden, is based more around IBM's marketing ethics than legal requirements. "We had an opt-in for e-mail long before the [EU electronic communications data protection] law was passed," she says. And in that respect, the EU's 2002 directive (which requires prior consent from consumers for all forms of electronic marketing) has not had a major impact on IBM's marketing practices. "As we already had the opt-in, we didn't have to change our entire business procedures."

Von Reden explains that the global approach on marketing choice is also reflected in the way IBM deals with the data protection statements that appear on data collection forms. "We have a worldwide format, but where necessary we adapt it to local requirements," she says. "Take the Italian law, for example, where a reference to the data protection controller is required, or the Polish law where a reference to the [data protection] law is necessary." While the main content of the notices are the same, whichever country you are located in, to be fully compliant, von Reden says companies need to factor in the small variations between national laws.

Compliance controls

With a standard policy for privacy protection in place, IBM has put in place a range of technical and management controls to ensure that the policy is adhered to. Training, says von Reden is a key element for all employees involved in the collection and use of data. For example, call centre staff are instructed on what privacy notices and choices they are required to give when responding to telephone enquiries. The idea is that consumers receive the same level of detail at every touchpoint throughout the organisation, whether they are filling out an online registration form, responding to a magazine advertisement, or calling a customer services centre.

For marketing departments, von Reden explains that staff are provided with tailored training programmes based around the local law and the

IBM compliance controls

- Data protection training for all staff handling personal data.
- Marketing materials vetted by legal department.
- Data privacy instructions to application designers.
- Data Privacy Review boards to ensure that new applications meet data privacy requirements and national laws.
- Privacy enhancing technologies to scan online data collection forms for compliance.
- Self-assessments and data protection audits.
- All marketing lists screened against an internal global opt-out database.
- Tailoring global policy to reflect local variations in data protection law.

IBM's corporate privacy instructions, (based on the OECD principles). These instructions cover marketing-related areas such as notice, choice, access to data, accuracy and data limitation, as well as security-related issues.

These instructions help to ensure that all marketing initiatives meet IBM's data protection policy. A further safeguard requires that marketing material be vetted by the legal department so that non-compliant material does not slip through the net.

To ensure compliance levels are maintained, data protection compliance requirements are inserted into the self-assessment checklists that every IBM marketing department, every brand and solution unit (essentially every organisational entity of IBM) has to fill out on a bi-annual basis. This is then followed up by an internal audit team to ensure that any compliance gaps have been found and fixed.

Privacy technology

In companies with a large online presence reaching across thousands of web pages, technology can play a vital role. Rather seeing it as an additional compliance cost, von Reden argues that privacy enhancing technologies "make life easier" when it comes to maintaining compliance. "In a company as big as ours, how can you find out whether they [web pages] have all complied to the same standard? You can't. It's much more expensive to put people in place to crawl through the data."

One of the tools IBM uses is a web monitoring programme developed by Watchfire (www.watchfire.com) which scans its corporate website for pages that collect personal data. It then flags up non-compliant pages, for example, if an online data collection form does not have the correct opt-in/opt-out choices or fails to provide a privacy statement. The data protection department will then issue the relevant instructions and remedies to the team responsible for posting up the web pages. As a final measure, says von Reden, "if they don't comply, then we kill the URL."

Key challenges

"In a company as big as IBM with so many different business units, to get everybody to adopt the worldwide standard that is required, takes a team effort," says von Reden. The sheer size of the company – IBM operates across 164 countries and employs over 300,000 staff – presents a huge challenge when trying to instill the same standards across different countries, business units and job functions. The key, she says, is to "take a centralised approach to compliance" but at the same time communicate to staff that they bear the responsibility if things go wrong. "Here at IBM, everybody knows it is his or her task to make sure that their business unit is compliant with the law."

While IBM, like many multinationals, favours a global standard for privacy compliance, variations in national laws prevent it from fully achieving that goal. Von Reden argues that there is still a need for greater harmonisation between European data protection laws. In the near future, she hopes to see the European Commission and national regulators introduce measures that will enable organisations to operate more effectively, through the development of initiatives such as European codes of conduct, centralised processes for notification and consistent criteria for data collection notices.

Overall though, IBM's compliance strategy appears to have been a success in Europe. A combination of high standards on marketing choice, coupled with strong internal controls has meant that the company receives only a handful of privacy-related complaints each year – which, considering the size and profile of the company is impressive.