7 Essential Steps for Designing Privacy into Technology

Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
fax:416-325-9195
www.ipc.on.ca

Define privacy expectations of the public and identify legislated requirements.

Develop privacy policies and principles.[1]

Undertake an assessment of human and informational resources with a focus on personally identifiable data (collection, processing, management, flows and storage).

Undertake a threat risk assessment by completing a Privacy Impact Assessment.[2]

Deploy methodology for privacy risk management at the systems level.[3]

Introduce the rules and controls developed in the previous step at the source code level.

Deploy and audit, through a model of continuous improvement. Review expectations and requirements.

[1] Privacy Diagnostic Tool - www.ipc.on.ca/english/whatsnew/newsrel/08601nr, Electronic Service Delivery: Privacy Standard - www.gov.on.ca/mbs/english/fip/pub/esd1, Code of Fair Information Practices - www.cdt.org/privacy/guide/basic/generic.

[2] Some useful examples of PIA are as follows: Management Board Secretariat's Privacy Impact Assessment - www.gov.on.ca:80/MBS/english/fip/pia/pia.pdf, "The Value of Privacy Engineering" by Steve Kenny and John Borking - elj.warwick.ac.uk/jilt/02-1/kenny.html

[3] Methodology should include the development of architecture rules and controls around collection of personal information, linkability, access, use and accountability as well as incoporating the delineation of business processes in terms of data. The methodology rules should be dependent on data type (level of sensitivity etc.).

Graphic Design: Ian Kuba, k Design Inc., kdesigninc@yahoo.ca