IT GOVERNANCE NETWORK

POPI: The role of the Information Officer in System Development

Complying with the Protection of Personal Information Act

The Protection of Personal Information Act specifies that the duties and responsibilities of the Information Officer include the encouragement of compliance, by the body, with the conditions for the lawful processing of personal information, deal with requests made to the body by data subjects, work with the Regulator in relation to investigations conducted pursuant to the requirement for prior authorisation from the Regulator and otherwise ensure compliance by the body.

Information Officer's Role in System Design

The information officer has two important roles regarding system design. The first is to give advice and guide responsible parties about compliance with the conditions for the lawful processing of personal information. The second is to confirm compliance with the conditions for the lawful processing of personal information.

To be effective, information officers need to be involved from the very beginning of any system design and will require access to information about the business requirements, system design, system management, service delivery, information security and the related privacy concerns.

Information officers will need an appropriate level of detailed knowledge and understanding of the data processing as well as access to the facilities, system components and information about the design and operation.

System development

For each individual module (or project milestone) in a development programme, the information officer should confirm with the project team that the agreed-upon implementation of the module complies with the conditions for the lawful processing of personal information.

Typical tasks that involve the information officer are:

- Documenting personal data-relevant business processes
- Defining the master data
- Determining the reporting system
- Examining the information flow of personal data, application interfaces and data flows to other systems
- Establishing personal information processing criteria
- Evaluating the user authorisation concept
- Evaluating test plans
- Defining migration and legacy data transfer.

Reliability of Information Officers

Information officers have a long term responsibility to the responsible parties, data subjects and the regulator for ensuring that the design of systems results in the lawful processing of personal information. The advice information officers give to system designers needs to be reliable so that the choices they have are correctly evaluated and appropriate decisions are made regarding the processing of personal information.

Often system designers and service providers focus only on getting systems to work well at solving a particular problem or delivering a specific service. They forget that an important property of processing personal information is to do so lawfully and therefore protect individual rights, enable intervention and inspection the data processing system, have it changed, and if necessary, shut off the system completely.

Privacy Design Consideration

During the course of processing, data is stored in the internal random access memory (RAM) and then swapped out of memory and cached to temporary storage locations. Regularly transient data, system dumps and log files are created. Inevitably this increases the effort to effectively erase data as soon as they are not necessary, and to make certain "deleted" data cannot be reconstructed.

Too often data processing hinges on the use of real names and unique personal identifiers when every day practice includes the use of nicknames or no name at all. Pseudonyms and anonymity provide system designers with alternatives to using personal data that is owned by third-parties.

While normalising database fields and tables minimises redundancy and eases maintainability, these benefits could be nullified if privacy is lost through poor database design.

When asking data subjects for consent, incomplete information is frequently the default and transparency is limited. People and organisations are often asked to commit themselves to more than really necessary. Privacy policies and notices are not crafted to be exact and complete. Privacy risks are increased through sloppy system descriptions and unclear responsibilities. Operators that do not provide the exact documentation by default and avoid transparency will increase the cost of assurance.

Function creep widens the scope of data processing beyond the original purpose. It violates the condition of binding the processing of personal data to a specific purpose. Avoiding context-specific identifiers will limit the risk of function creep and increases contextual integrity.

Location of data does matter, particularly in law. Very often the jurisdiction is determined by the location of an action or the place of business when a service is being provided. Data subjects in South Africa have a number of rights that the Protection of Personal Information Act protects, as do data subjects in Europe and other jurisdiction. Processing personal information across borders increases the risk of non-compliance with foreign jurisdiction privacy obligations.

Can it be proven to the data subject that a deletion of data initiated by the data subject actually includes all generations of copies and versions of backup files? Processes need to be arranged to enable intervention. Often problems occur because the system design did not consider the full lifecycle of the data. It might appear to be more important to provide a quick solution, be early on the market and create advantages, than to plan ahead and develop proper solutions that enable privacy.

www.itgovernance.co.za cell: 0825588732 info@itgovernance.co.za