IT GOVERNANCE NETWORK

Protection of Personal Information and Big Data

COMPLYING WITH THE PROTECTION OF PERSONAL INFORMATION ACT

Addressing the privacy challenges of big data is first and foremost the responsibility of those collecting and using personal information. "Responsible parties must secure the integrity and confidentiality of personal information in their possession or under their control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information" – Protection of Personal Information Act.

Protecting Personal Information in BIG DATA

Before reaping the benefits of Big Data, "the responsible party must identify all reasonably foreseeable internal and external risks, establish and maintain appropriate safeguards against the risks identified, regularly verify that the safeguards are effectively implemented and continually updated in response to new risks" – POPI Act.

Adequate principles, policies, frameworks, procedures and practices are necessary to support the achievement of the business strategy through big data. There is a real danger that individuals may be judged not because of what they've done, or what they will do in the future, but because inferences or correlations drawn by algorithms suggest they may behave in ways that make them poor credit or insurance risks, unsuitable candidates for employment or admission to schools or other institutions, or unlikely to carry out certain functions. There is also considerable risk that using big data will breach privacy obligations and legislation.

Operational Risk

Predictive analytics of big data is a tremendous tool when used and applied correctly. The collection of apparently unlinked data may appear harmless by itself, and its predictive powers could create value through increased knowledge and greater predictability of expected outcomes which drives competitive advantage with better service levels, increased revenues and lower costs. But at what risk to the responsible parties involved and their organisations?

Whilst it may be technically feasible to explore and access data stored in many systems and silos for the purpose of enhanced decision-making, it will not be legal unless the eight conditions for the lawful processing of personal information are adhered to. The benefits of big data could quickly evaporate through loss of reputation, trustworthiness and customers' loyalty, as well as financial settlements, administrative fines, penalties and civil damage claims.

Making use of big data before proper risk assessments are complete and effective controls are applied could result in the exposure of personal data in ways that are unlawful.

Big Data Risks

- Indiscriminate collection of personal information
- Failure to first obtain consent from data subjects
- Collection of unreliable data
- Not informing data subjects about the collection and intended use of their data
- Not providing meaningful consumer choice – not contrary to personal preference
- Preventing data subjects from participating in the review of their personal data
- Cross-border sharing and processing
- Multiple layers of role players with unclear accountability
- Ineffectiveness of use restrictions after a breach occurs
- Impact of a data breach usually involves large data volumes
- Behind the scenes profiling – secondary processing.

Questions to ask before using Big Data

- Are we exploiting individuals' right to privacy?
- Can we trust our sources of big data?
- Do we have the right tools to meet our big data privacy requirements and fulfil our legal obligations?
- How do we verify the authenticity of the data?
- Can we verify how the information will be used?
- What choices do we have regarding big data privacy?
- Will we record the consequences and actually use that information to improve our big data information gathering analysis and decision-making processes?
- How will we protect our sources, our processes and our decisions from theft and corruption?
- Are we collecting information without exposing the enterprise to legal and regulatory sanctions?
- What measures are in place to ensure that employees keep stakeholder information confidential during and after employment?

Generally accepted Big Data Practices

- Using appropriately secure and reliable infrastructure
- Anonymising or de- identifying personal data
- Applying filtering, cleansing, pruning, conforming, matching, joining, and diagnosing at the earliest touch points possible
- Avoiding incomplete information, poor decisions and bias
- Tracing data elements back to the source
- Maintaining adequate, relevant, useful and current big data related policies, processes, procedures and supporting structures
- Maintaining privacy notices with details about all intended uses, an individual's access rights and ways to address incorrect data
- Providing easy data subject access to review and correct information that has been collected about them
- Performing appropriate data destruction within a comprehensive data management policy, clearly defined disposal ownership and accountability
- Providing continuous education and training about big data policies, processes and procedures.

Safeguarding Data Subjects

- ❖ Privacy by design
  - ■ Avoid weak infrastructure
  - ■ Avoid data duplication
  - ■ Avoid involuntary revelation of sensitive information
  - ■ Avoid the users losing anonymity
  - ■ Preplanning responses to privacy breaches
  - ■ Avoid contravening the law
- ❖ Simplified choice
  - ■ Inform data owners who is collecting their data
  - ■ Allow data subjects to take control over their data
- ❖ Greater transparency
  - ■ Move commercial use of data into the spotlight.

www.itgovernance.co.za info@itgovernance.co.za