FIVE ESSENTIAL TIPS TO GUIDE CONTRACTING OF DATA PROCESSORS

Organizations as part of their business may contract data processors. A data processor is any person, external entity service provider, or thirty party contracted to process personal data on behalf of the organization.

Privacy laws require organizations to ensure that all their data processors have adequate measures to establish and maintain the confidentiality and security measures necessary to protect the integrity of personal data. Organizations should therefore issue contracts to data processors before any processing takes place.

As per best practice, organizations should undertake the following when considering the use of data processors:

1. Include requirements for protecting personal data within the request for proposals, terms of reference, software design specifications as mandatory areas for interested third parties. These requirements enable personal data protection at the start other than treating it as a 'bolt-on' activity after or near the implementation!
2. Perform a Data Protection Impact Assessment (DPIA) where the processing of personal data poses a high risk to the rights and freedoms of data subjects. At the minimum, the DPIA includes a systematic description of the processing, assessing the risks to the personal data and the measures to reduce any identified risks. An example of when to use the DPIA is when an organization considers a new service or innovation that involves sharing sensitive personal data with third parties.
3. Ensure the contract with the third party provides for the following minimum areas:
   a) Clauses that specifically require the data processor to implement and maintain the appropriate technical and organizational measures to protect personal data against any breach or misuse. Privacy laws require data processors not to disclose personal data unless required by law or in the course of the discharge of a duty.
   b) Organisations should include stricter security measures where sensitive or special personal data is involved, such as religious, philosophical beliefs, political opinion, financial information, health status, or medical records of an individual
   c) Require data processors to inform and seek your guidance for any sub-processors.
   d) Require data processors to notify the organization in case of any data breach that exposes personal data. The notification should include the requirement for the processor to collaborate in case of any audits or investigations following a breach.
   e) Description of the means to achieve and maintain the secure transfer of personal data between the organization and the controller for both electronic and paper records.
   f) Provisions for data retention periods and end of contract terms that specify how personal data will be deleted or disposed. This should also include establishing and maintaining evidence that the data processor no longer retains personal data after contract expiry. Disposal of personal data may be a challenge where organizations use third-party platforms to process personal data, such as Software as a Service. Therefore, organizations need to seek professional advice from data protection and privacy experts to cover all grounds.
4. Perform due diligence to ascertain the effectiveness of the technical and organizational measures that the data processor has implemented. Organizations should also check where data processors store data to ensure compliance with Privacy laws that define acceptable countries or territories. This due diligence enables an organization to meet

the obligation of a data controller not to contract a data processor unless they have implemented the security measures specified under Section 20 of the Act.

5. Include disclosure of such data processors in the organization’s privacy notices. The disclosure should list the data processors, reasons why they are used, categories of personal data they process, and security measures to protect the confidentiality and integrity of personal data.