R2P week 26:

Elements of third-party contracts checklist

Create your own customised checklist to identify certain elements of third-party contracts such as privacy compliance, breach notification, sub-contracting, etc. to ensure:

- the contract requires the third party to meet privacy compliance requirements;
- the contract requires the third party to notify in the event of a breach;
- the third party trains their employees for general awareness and role-based as needed;
- permissions regarding subcontracting: if unable to limit subcontracting, ensure a requirement to pass on all privacy provisions;
- right to audit or to access a third-party audit report;
- description of data transferred overseas: permissible reasons and protections.

Procuring organisation may have specific standards and processes for vendor selection. A prospective vendor should be evaluated against these standards through questionnaires, PIAs, and other checklists. Standards for selecting third parties may include:

- Reputation: A third party's reputation with other companies can be a valuable gauge of the third party's appropriate collection and use of personal data. Requesting and contacting references can help determine a third party's reputation.
- Financial condition and insurance: The third party's finances should be reviewed to ensure the third party has enough resources in case of a security breach and subsequent litigation. A current and sufficient insurance policy can also protect the procuring organisation in the event of a breach.
- Information security controls: A service provider should have sufficient security controls in place to ensure the information is not accessed without authorisation, lost or stolen.
- Point of transfer: The point of transfer between the procuring organisation and the third party is a potential security vulnerability. Mechanisms of secure transfer should be developed and maintained.
- Disposal of information: Appropriate destruction of information in any format or media is a key component of information management for both the contracting organisation and its third parties. [The Disposal Rule under the Fair and Accurate Credit Transactions Act of 2003 (FACTA, USA) sets forth required disposal protections for financial institutions. The Disposal Rule requirements provide a good baseline for disposal of personal information more generally.]

- Employee training and user awareness: The third party should have an established system for training its employees about its responsibilities in managing personal or sensitive information.
- Third party incident response: Because of the potentially significant costs associated with a data breach, the third party should clearly explain in advance its provisions for responding to any such breach with the cooperation needed to meet the organisation's business and legal needs.
- Audit rights: Organisations should be able to monitor the third party's activities to ensure it is complying with contractual obligations. Audit needs can sometimes be satisfied through periodic assessments or reports by independent trusted parties regarding the third party's practices.
- Policies and procedures: Third parties are generally expected to have documented policies around the handling of personal information in their organisation, as well as procedures for dealing with individual rights, data breaches, etc.
- Privacy Officer: The third party should have a PO who is responsible for the organisation's management of personal information.

R2P Week 26: ELEMENTS OF THIRD-PARTY CONTRACTS

Business Unit/Process		Committee Member	

CHECKLIST

In the third-party contract, we have clearly identified:

☐ the specifics regarding the type of personal information to which the third party will have access at remote locations;

☐ third-party plans to protect personal information;

☐ third-party responsibilities in the event of a data breach;

☐ the manner in which the third party will dispose of the data upon contract termination;

☐ limitations on the use of the data that ensure they will be used only for specified purposes;

☐ rights of audit and investigation;

☐ liability for data breach.

The above list provides a few examples of the kind of information you may want to consider for third party contracts. It is not an exhaustive list. We encourage organisations to customise it to fit their needs.
Contract language should be written to call out privacy protections and regulatory requirements within the statement of work and then mapped to service-level agreements to ensure there are no questions about the data privacy responsibilities, breach response, incident response, media press releases on breaches, possible fines, and other considerations, as if the third party/vendor were part of the organisation.