International Bar Association
the global voice of the legal profession

Legal Practice Division (LPD)

Dear friends,

This month work has focused on a few transactions involving third parties, which provided me valuable insights for a presentation on a privacy panel titled 'Managing Third-Party Vendor Risk: Tips for Protecting Your Business.'

I was assigned the discussion on negotiation and drafting of third-party contracts. As technology lawyers, we are familiar with data and privacy issues in third-party contracting, which arise at all stages of the contracting process. So, I decided to break up the risk checks and balances into the before, during, and after stages. I share some of my thoughts here with you.

Before the agreement is signed

While it is difficult, at the initial stage, to ascertain the privacy and cybersecurity risks that may arise in the future, it is, nevertheless, important to identify risk tolerance first. Tolerance for reputational damage, fines and fees, remediation, class actions, and private rights of actions.

Third-party risk management (TPRM) helps manage vendor risks more effectively. This analysis includes what data will be processed, who will process it, where it will be processed, how it will be processed, and why it will be processed. Further, it defines whether the vendor's responsibilities and roles in respect of data and cybersecurity are clearly articulated, as also which laws, regulations, and standards are applicable.

A theme that I emphasized was the obligation of parties to coordinate, cooperate, and communicate on all aspects of privacy and cybersecurity, including changes in landscape. It is ideal to have a cross-functional team that covers procurement, vendor risk management, IT, security, and legal aspects at the outset of a third-party engagement. Joint governance process not only helps address risks in a coordinated fashion but also mitigates future risks.

During negotiations

It is important to steer towards a common understanding of business objectives, covering not just the relationship, but also the intended value provided by the third party. In fact, it is a plus to include all expected security controls in the original Request for Proposal (RFP).

Standardisation of language, definitions, and boiler plate clauses helps in drafting and subsequent interpretation. Divergent assumptions about data autonomy versus conformity may create problems when any such difference is identified late in the game. The best choice is to negotiate with a focus on a dynamic rather than a static relationship.

‘Which template to use’ is probably a phrase commonly heard when negotiations begin. Irrespective of whose template is used, the following topics are important to consider:

- How the parties will work together. The contract should outline the broad process expectations of parties' interaction: communication norms; handling unforeseen events; dispute resolution; renegotiation options; etc.
- Third parties to follow clients’ specific written instructions in respect of processing data
- Third parties to comply with amended terms reflecting the client’s response to any amendments in law
- Attention to every aspect of data collection, transfer, use, storage, and retention - not only for data localisation needs, but also for recognising access, correction, and erasure rights of data subjects, as well as to understand where data will be stored and how it will be destroyed
- Identifying the parties beyond the third party
- Ascertaining how the relationship will end: set contours for a graceful end and a seamless transfer
- Defining *force majeure* to include unauthorised access or distributed denial-of-service attacks

After execution of the agreement

Execution of a service-level agreement is just the first step to addressing data risk. Every third-party posture and relationship is required to be reassessed on a regular basis, particularly whenever there is a scope change, technology change, or a security incident. If standards are upheld at each stage of creating a relationship, third-party relationships become assets, not a liability, to be feared.

Now, of critical importance is cooperation, coordination, and communication, including providing information to comply with privacy and cybersecurity laws, any changes therein, and discussions, in good faith, on reducing costs related to changes in compliance obligations.

Regular audits and assessments help parties remain on top of any situation. If a data breach were to happen, all parties should be brought into a single-incident management process that investigates, contains, reports, and remedies the breach.

When a contract ends

While contracts eventually terminate, the requirements for data care and protection generally continue. The worst possible time to address the high pressure, complex, sensitive, and emotional issues associated with data protection is during a termination process! Rather, a vital part of contracting is appropriate termination planning, which ensures a successful process transition to the client or new vendor. Any neglect in such critical planning runs the risk of business disruption.

When a contract ends, or is terminated, parties need to brace themselves for the inevitable questions relating to data and its privacy. Is there any personal data? Do data subjects have the right to opt in or opt out of the processing of their data? Is the data being transferred across borders? What privacy laws apply? These are just some of the bewildering questions that arise at the end of a third-party relationship.

No third party has the right to withhold access to data under any circumstances; rather, the client must know where the data is, where it is going, and how they can get access to it in a form they can use. The client retains ownership of all its data and confidential information.

The doubts get compounded in multi-vendor arrangements. What happens when only one of the multi-vendor relationships ends? If one vendor depends on another for secure encrypted data transfers, and its agreement ends, this may be a trigger for liability.

The best future proofing tool in an evolving privacy and cybersecurity ecosystem is, perhaps, privacy by design. Principles of privacy by design should ideally be integrated into procurement, contract negotiations, contract administration, and company policy.

We welcome your thoughts on third-party contracts that you have negotiated. Do share these observations and related anecdotes, if any.

Those of you who are heading for a summer vacation, my good wishes for a relaxed time.

Warm regards,

Sajai Singh

Co-Chair, IBA Technology Law Committee
sajai@jsalaw.com