DATA PRIVACY: HOW SECURE IS SECURE?

Today's reality

Anthony Gonsalves booked a stay at a hotel online and provided his credit card details to make the necessary payment. For future convenience, Anthony saved his credit card details on the hotel's website. The hotel continued to retain his credit card details along with the credit card details of other guests for a number of years. Recently, the hotel's cloud server was under cyber-attack and the credit card details of Anthony along with other guests were up for grabs in cyberspace. This incident highlights today's reality- Your identity can be sold for petty cash. The more personal data we share, the more susceptible we are to data breach. Information is the new currency and potentially, every data cloud has its black lining.

Recent events have only underpinned the extent to which personal data can be violated and misused. As per Citrix ShareFile, healthcare is the most vulnerable industry in the US, with technology, retail and finance industries taking second and joint third places respectively.[1] Even India has faced its fair share of data breaches. Zomato reporting a theft of approximately 17 million email addresses being just one example.

In response to such threats, Governments world over are stepping up to tackle this threat and compelling businesses to be more responsible for securing the personal data of individuals.

…..Meanwhile Data Privacy & Protection: The India Context

India presently does not have a comprehensive data protection legislation. The main enactment that deals with protection of data is the Information Technology Act, 2000 and the rules framed thereunder. Under the provisions of IT Act, the IT authority has adjudicated a number of cases related to cyber fraud and data breaches. In one such significant case, in 2013, the Maharashtra's IT secretary directed Punjab National Bank to pay INR 45,00,000/- on a complaint, where a fraudster had transferred INR 80,10,000 from the complainant's account after the complainant responded to a phishing email. The complainant was asked to share the liability since he responded to the phishing mail, however, a more important point to note is that Punjab National Bank was found negligent due to lack of proper security checks against fraud accounts opened to defraud the complainant. This incident only proves to highlight the need for businesses to be more responsive to prevalent data security threats.

In keeping with the proactive approach to data privacy by government's worldwide, the Indian Government is also in the process of providing for a more robust legislature. The Data Protection bill by the Justice Srikrishna committee is now keenly awaited by corporate India. The two pending cases before the Supreme Court which are likely to have an impact on the legislature are (a) the challenge to the Aadhaar Act, and (b) the case filed by Karmanya Singh Sareen challenging the change in privacy policy of WhatsApp Inc.

[1] *https://www.fastcompany.com/40527767/these-industries-are-the-most-vulnerable-to-data-breaches-in-the-united-states*

© Economic Laws Practice 2018

Best Practices Recommended….

Given the scenario of high data privacy compliance globally (and potentially very soon in India) the pressing need is to understand some best practices which organisations within India can adopt to mitigate data privacy risks within their organisations.

Immediate Next Steps….

- The first is to conduct an extensive audit on existing privacy policies and procedures. Being prepared in advance with checklists of requirements met and equally with lacunae which need to be addressed, will ultimately ease and help streamline the data protection requirements once the Data Protection bill gets adopted.
- Organisations should look at implementing standard operating procedures ("SOPs") to meet consent requirements of data subjects as well as to deal swiftly with data breaches. It may be helpful for such organisations to have in place dedicated teams to ensure compliances with data privacy laws.
- Cross border data transfer policies vary from country to country. In case of cross border data transmissions, a specialised team should be engaged to ensure local law compliances. The foremost issue with regulating cross border data flows is with determining the threshold factors based on which the transfer will be permitted. For example, cross-border data flows to a jurisdiction with lower levels of privacy protection can undermine domestic privacy protection. This creates an incentive for regulators to restrict cross-border transfers of personal information.

> The European Union's General Data Protection Regulation ("GDPR") prevents transfers of personal data to another jurisdiction that has not been deemed by the EU to have adequate privacy protection. The European Court of Justice has found that a finding of adequacy requires the other country to provide privacy protection that is "essentially equivalent" to that found in the EU.

- Certain countries have robust data localisation norms. Indian companies which have subsidiaries in different jurisdictions should be mindful of such requirements before transmitting data to local servers in India.
- Many executives may be surprised to learn that one of the most frequent causes of data breaches is employee error, and not just employees in the IT department. Errors could be as simple as failing to lock a door, replying to phishing emails, sending emails to the wrong id's. A careless mistake can cause massive damage. Training for employees is therefore crucial in a cohesive data security plan.
- Data portability is a right of the data subjects under certain legislatures. Organisations should be ready to honour the requests for transmission.
- A viable security breach response plan helps in identifying the steps required to be undertaken by the organisation to restore the damage caused. The incident response plan must be unique and tailored to the working nature and operational requirements of each business. If these aren't considered, the plan holds minimal value. It is important to list the most valuable assets and clearly state where these are located- be it physical or virtual. Once listed, the plan must consider the risks that would be posed if those assets were to be seized during an attack.

And…Important points to take note

- According to McAfee insiders are responsible for 43% of data breaches. What then are the steps can one adopt when the problem lies within. Bring your own device ("BYOD"), remote working, storing data on shared files, weak firewalls and passwords are all possible avenues for inadvertent insider data leaks. To tackle this issue, only those employees that need to work directly with such sensitive data could be given partial or complete access, depending upon the requirements. Along with granting limited access to employees, organisations could give additional protection to data which is sensitive in nature by implementing strong data security policies and introducing network logging anytime an employee wants to access the data.

> UIDAI has issued guidelines on security for storing Aadhaar numbers. Reference key mapping has been mandated with emphasis on the Aadhaar data vault where the Aadhaar number and any connected Aadhaar data will be stored. It has further been mandated that access to the data vault must be highly regulated.

- Data should not be stored beyond a certain time period- relevant for the purpose for which it was collected.
- Collecting data beyond the scope of regulatory requirements/contract requirements should be avoided.
- Former employee data retention policies must be thoroughly reviewed. It is appropriate to retain former employees' personal data up to the expiry of the statute of limitation period provided by local laws.
- Organisations should not ignore the request for deletion of personal data by the data subject. Right to forgotten is an important right under certain legislatures like GDPR.

…..Staying one step ahead

Companies will need to be one step ahead and be adequately prepared for the new legislature. The plinth will be a cohesive data privacy strategy supported by, technology, operations and people. There will be a paradigm shift in how organisations function. Data cannot be taken for granted any more.