SHRI EDUCARE LIMITED

FEBRUARY 2021

DATA PROTECTION LAWS

Summary of the Indian Scenario

PREFACE

Have you ever wondered how the suggestions about your next purchases i.e. televisions, mobile phones, and travel packages to your favourite destinations, magically start appearing on your social media accounts just few hours after you had that first talk about them with your family? Or how making just one e-commerce transaction leads to numerous telemarketing calls aiming to sell you customised health insurance plans, real estate deals, investments options and even matrimony website subscriptions, tailored to your age, gender, location and other traits unique to you? Or why do almost all e-commerce start-ups have exclusive offers/ freebies on signing-up as a new customer?

Further, do you really agree or even care to read the Privacy Terms and Conditions while clicking “I Agree” in a hurry of signing up for any product/ service?

If any of the above questions got you curious, please read on to know the value of the most precious asset of this century and “who is the product for sale in this world of no free lunch”.

Also, you also get the answer to a billion dollar question – how do your favourite start-ups/ brands and social media companies earn even by keeping their services free for you, forever.

WHAT IS DATA?

Among other important definitions covered under the Information Technology Act, 2000, the definition of **information** can be interpreted to include **Data**, texts, images, software etc. and **Data** includes a representation of information, knowledge, facts, concepts or instructions processed in a computer and stored in a soft or hard copy.

Examples of data are:
(a) Internet browsing history
(b) Shopping history/ pattern
(c) Medical reports/ history
(d) Articles, news, movies of your interest
(e) Names of your bankers, loan providers etc.
(f) Age, sexual orientation, beliefs, location history, connections etc.
(g) Biometric information

What is Personal Information/ Data?
Any information of a natural person, available with a body corporate, directly or indirectly capable of identifying such person.

E.g. PAN of an individual is Personal Information, whereas PAN of a company is not.

Why is it important to protect Personal Information/ Data?
To prevent misuse i.e. any usage beyond the purpose for which such data has been provided by the information provider.

LEGAL FRAMEWORK: DATA, PRIVACY AND PROTECTION

(A) Existing statues

Directly related statutes:

- The Information Technology Act, 2000
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Indirectly related statutes:

- Indian Penal Code, 1860
- Copyright Act, 1957
- Aadhaar Act, 2016
- Constitution of India, 1950
- Indian Contract Act, 1872
- Right to Information Act, 2005

(B) New (additional) legislation (proposed)

- Personal Data Protection Bill, 2019

SOME GUIDELINES FOR COLLECTING, RECEIVING, STORING, PROCESSING, AND USING THE PERSONAL INFORMATION/ DATA

1. Seek and/ or collect only that information/ data which is directly necessary for the main purpose of association between the associating parties. No other information should be collected.
2. Obtain written consent from the information provider for collection, usage and/ or transfer of such information/ data, for the specified purpose, alongwith sharing the details of recipient.
3. Option to reject/ revoke such consent should be made available.
4. The information collected should be available for viewing by the information provider.
5. The information collected should not be stored for a period beyond the completion of purpose, except as required under law.
6. International standard IS/ISO/IEC 27001 or such other standard notified by government maybe used to ensure compliance of having reasonable security measures in place.
7. Formulate and implement a Privacy Policy governing the aspects related to collection, storage, processing and usage of such data.
8. Publish the Privacy Policy on website of the Body Corporate.
9. Statement of security measures and policies should be clearly and easily accessible (e.g. Privacy Policies written in tiny font can be challenged)
10. Appoint a Grievance Officer whose name and contact details should be published on the website.
11. Grievances must be redressed within one month of receipt.

SOME MANDATORY CONTENTS OF A PRIVACY POLICY

1. Nature of Personal Information/ data to be collected.
2. Purpose of collection and usage of such information/ data.
3. Time period for which such information/ data shall be maintained.
4. Detailing of Grievance Redressal mechanism.
5. Appointment of a Grievance Officer
6. Exceptions where the data transfer/ disclosure shall not amount to breach of the Policy.
7. Data security measures implemented by the data recipient for preventing misuse by insiders or any third party.

THE AADHAAR JUDGEMENT: A LANDMARK CASE ON DATA COLLECTION AND PRIVACY

Justice K. S. Puttaswamy (Retd.) vs. Union of India, (2017) 10 SCC 1

Brief facts

A retired High Court Judge K.S. Puttaswamy filed a petition in 2012 against the Union of India before the Supreme Court challenging the constitutionality of Aadhaar because it is violating the right to privacy and to determine whether or not the right to privacy was guaranteed as an independent fundamental right under the constitution of India.

Issues

Amongst other issues at hand, the judicial bench was given to decide the constitutional validity of Aadhar that whether it infringed the Right to Privacy and whether private entities could use the biometric and other information captured under the Aadhar initiative.

Judgement

In the year 2017, The Supreme Court decided that the Right to Privacy was an integral part of the fundamental rights under the Indian constitution and that every individual should have control over commercial use of his/ her personal information. Therefore, the Court struck off certain provisions of the Aadhar Act as unconstitutional and void, in turn making Aadhar an optional KYC document and not a mandatory submission. Also, as a consequence, it was mandated that though private entities could also use the information and biometrics captured under Aadhar, the same can be done only under express consent of the Aadhar Holder.

Consequential orders

Among the earlier requirements to link Aadhaar numbers to PAN, Bank Accounts and mobile numbers, only the linking of Aadhar with PAN was held to be valid, since it was based on a law, serving a legitimate state interest.

NEED OF A NEW DATA PROTECTION REGULATION

1. The existing framework doesn't have a robust mechanism of governing information/ data protection offline.
2. In the year 2019, Computer Emergency Response Team (CERT) reported around 3.13 lakh data breaches in just one year.
3. Regulations governing the protection of personal data are scattered across various legislations like the Contract Act, Information Technology Act, Sensitive Data Rules and Aadhar Act etc.
4. No governance mechanism for data exchanged over Social Media websites and other e-platforms.
5. General Data Protection Regulation (GDPR) restricts free transfer of data from the European Union countries to the countries which do not comply with certain data protection measures' adequacy requirements.
6. There is a need to shift from penalty based regulation against data centres (for failure to implement data protection measures) to a law which recognises rights of the information providers.

CAMBRIDGE ANALYTICA/ FACEBOOK SCANDAL

A mobile based application called Cambridge Analytica collected its users' political and other interests, and other personal data including their Facebook friends' profiles by way of certain questionnaires and built their psychological profiles.

This data got compromised and was sold to political parties in the US for targeted advertising, thereby assisting political campaigns of Ted Cruz and Donald Trump in the year 2016.

This was claimed as the "largest known leak in the Facebook history".

The information about the data usage later got public in 2018 during interview of a former Cambridge Analytica by the New York Times.

As a result, UK Information Commission Offices imposed heavy penalties on Facebook for absence of enough data protection measures.

INSIGHTS INTO THE PERSONAL DATA PROTECTION BILL (PDP BILL)

1. The definition of personal data is wider, more exhaustive and covers even data collected offline, which can identify a natural person.
2. Defines the term 'Data Fiduciaries' and their obligations.
3. Introduction of different classes of data fiduciaries.
4. Data localisation concept has been introduced, wherein non-critical data is allowed to be transferred and stored outside India, with a copy retained in India. This was not allowed in the original bill moved in 2018.

Who: Data Fiduciaries include legal entities, individuals and the state. As against the current law, the government authorities and individuals collecting data have also been covered.

What: PDP Bill specifies the manner to collect, handle and process data, details the necessary data protection safeguards to be put in place, prescribes the requirement and contents of a privacy policy to be implemented by all data fiduciaries.

How: Transparency and Accountability: Governing Authority by the name of Data Protection Authority is proposed to be set up who should be notified of any instances of breach.

CLASSIFICATION OF DATA FIDUCIARIES

Guardian Data Fiduciaries: The collectors, handlers and processors of volumes of children data are assigned additional compliances and responsibilities.

Significant Data Fiduciaries: The entities which process data of large number of users are responsible for additional measures such as impact assessments and file periodic analysis with the authorities. These fiduciaries should get their data policies and collection methodologies audited periodically.

Social Media Intermediaries: These fiduciaries enable business or e-commerce transactions and include search engines etc. Power has been given to Data Protection Authority to identify such data collecting intermediaries which process data of large number of users online and/ or their dealing with data may have an impact on the electoral democracy or security or state.

RIGHTS OF DATA PRINCIPLES (INFORMATION PROVIDERS)

1. **Right to confirm** whether the given personal data is being processed or has been processed.
2. **Right to access** summary of the processing activities performed with respect to the personal data, identities of all fiduciaries who have got access to such data.
3. **Right to correction, completion or updation** of any errors and out-of-date informations.
4. **Right to erasure** of any information submitted earlier and whose agreed purpose of use has been completed.
5. **Right to be forgotten** is another way to revoke consent to use the information/ data submitted, which may include discontinuance of provisions of goods or services, for which such consent is a must.
6. **Right to data portability** means a right to obtain the information submitted in a copy or to request transfer of such data to some other fiduciary.

MISCELLANEOUS EXAMPLES

- **What happens if the confidentiality clause is not contained in the contract? Can the recipient make the proprietary information public in the absence of an NDA (Non-Disclosure Agreement)?**

  It is not mandatory to have a confidentiality clause written in each contract to prevent disclosure of proprietary information which is confidential by its very nature e.g. list of clients, future project reports, etc.

  Further, the recipient cannot disclose any trade secrets or other such confidential information obtained by virtue of its association with the disclosing party.

- **Can a husband obtain the Income Tax returns filed by his wife under the Right to Information Act?**

  No, the public authority is under no obligation to disclose any personal information having no relation to any public activity or interest.

FEW LEGAL OBLIGATIONS TO UNDERTAKE SECURITY MEASURES

1. As per **Section 43A of the Information Technology Act, 2000,** negligence of a body corporate which possesses or deals with electronic sensitive personal data to maintain reasonable data security measures, causing thereby wrongful gain/ loss, shall make him liable to pay damages to the aggrieved person.
2. As per **Section 72A of the Information Technology Act, 2000,** any person who has gained personal information of some other person, discloses such information to a third party, without obtaining discloser's consent and with an intent of attaining wrongful gain or causing wrongful loss, shall be punishable with imprisonment of 3 years and/or fine up till Rs. 5 lakhs.
3. As per **Section 57 of the Personal Data Protection Bill, 2019**, the maximum penalty that can be levied on a data fiduciary is Rs. 15 crores or 4% of the global turnover, whichever is higher, depending on the violation done.

FEW KEY DIFFERENCES BETWEEN THE GENERAL DATA PROTECTION REGULATION (GDPR) AND THE PERSONAL DATA PROTECTION BILL, 2019 (PDP BILL)

1. Localisation norms have been recognised in the PDP Bill but it is not so in the GDPR.
2. Performance of a valid contract constitutes as an exception of data sharing restrictions under the GDPR.
3. GDPR allows member states to fix consent age as 13-16 years, whereas Indian bill recognises only the adult age of 18 for such purpose.
4. PDP Bill recognises a right to revoke consent and prevent further disclosure of information, in addition to the right to erasure, as granted under both the laws.
5. PDP Bill includes the State in exception list whereby it is allowed to process certain non-personal data for the purposes related to policy formation.

RECAP AND CONCLUSION

Taking cue from where we began, if the questions in the preface have not got answered for you in the above contents, let us take them up again briefly.

The power behind Siri, Alexa or Ok Google's ability to give you personalised suggestions or making recommendations based on your personality lies in the data that you knowingly or unknowingly share with various entities sitting in each of your electronic devices through their mobile applications, be it your smartphone, smart television, and other smart home appliances, which are smart only because they know a lot more about you than you think they do.

Also, the services that are available to sign-up for free or the discounts offered to new customers, all of them charge you a cost i.e. your information and data, which is the most precious asset for the companies who are waiting to analyse your personality in order to gauge your needs.

This is done to ensure that the advertisements thrown at you are well targeted, reach the right audience at the minimum cost and see maximum conversions because the products/ services were offered to those who need them, and at the time that they need them.

Therefore, it is important that the government brings in regulations to keep a check on judicious use of such personal data and ensure that its usage does not bring harm and threats to the data owners and society at large.

REFERENCES

1. The Information Technology Act, 2000
2. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
3. Indian Contract Act, 1872
4. Personal Data Protection Bill, 2019

Web references:

1. www.mondaq.com
2. www.prsindia.org
3. www.indiacode.nic.in
4. www.meity.gov.in

Shri Educare Limited

Unitech Business Zone,
Tower- C, 1st
Floor,Nirvana Country,
Sector 50, Gurugram-
122018, India

www.shrieducare.com