UNFOLDING THE A-Z OF CYBERSECURITY IN INDIA: OPPORTUNITIES AND CHALLENGES

By - CA. (Dr.) Rajkumar Adukia
Mobile No.: 9820061049/9820061039
Email rajkumar@cadrrajkumaradukia.com

India has recognized the importance of cybersecurity amid the rapid digital transformation and increasing cyber threats. The government and various regulatory bodies have implemented several legal initiatives to strengthen cybersecurity and protect sensitive information. In this article we will unfold the a-z of cyber security. Keeping in mind our overdependency on the internet and the associated risks that comes along with it also the rising demand for cybersecurity professionals the author has made an attempt to provide you with ample of professional opportunities that the world of cyber security will provide. Together, we can navigate the digital landscape with confidence, ensuring a secure and resilient online environment for all.

I. Introduction:

In our modern age, the internet has revolutionized every aspect of life—from studying and working to shopping and entertainment. This digital transformation has undeniably simplified our daily routines, making information and services more accessible than ever. However, this convenience comes with significant risks, as the threats associated with cybercrime have proliferated in tandem with our reliance on technology. Consequently, the importance of cybersecurity has gained prominence, driving demand for skilled professionals who can safeguard our digital lives.

As our lives become increasingly intertwined with the digital realm, so do the vulnerabilities we face. Cyber threats, ranging from data breaches to identity theft, pose

serious risks not only to individuals but also to organizations and institutions. This has led to a critical need for cybersecurity measures to protect sensitive information and maintain trust in digital interactions.

Some core subjects the cyber field revolves around to:

1. E-commerce
2. Digital signature
3. Intellectual property rights more particularly Copyright and Trademark
4. The Information Technology Act, 2000
5. Evolving personal data protection bill 2019 , non personal data compliance regime
6. GDPR compliance
7. Personal data protection laws compliance
8. Non personal data compliance
9. Setting up strong cyber security department-compliance
10. COBIT compliance

11. Electronic Fund Transfer fraud
12. Credit card transfer
13. Cyber threat to personal data
14. Regulation of cyber crime
15. International cyber law regime
16. Online defaming
17. E-contracts
18. Privacy infringement
19. Industry wise specialization – banking, insurance etc.
20. Use of social media for business and professional growth

One can rightly assert that the new digital age is unfolding never ending professional opportunities scope for professionals like chartered accountants turning them into data protection specialist thereby adding value to their core area of expertise.

Few Lucrative professional opportunities in cyber security field

1. Advisory to Government department/organization/ministry
2. Advisory to web developers, private organizations
3. Consultant to e-commerce companies and other tech companies
4. Cyber Consultant to firms, bank, police department
5. Cyber security manager
6. Security architect
7. Cyber security analyst
8. Cyber assistant
9. Social media risk management
10. Social media activities audit
11. Privacy regulation audit
12. IT contract management assessment

13.IT investment program risk

The Role of Cybersecurity Professionals

Cybersecurity professionals play a pivotal role in creating a secure digital environment. Their expertise enables them to:

1. Assess Vulnerabilities: By conducting risk assessments and penetration testing, these experts identify potential weaknesses in systems and networks.
2. Develop Security Strategies: Professionals design and implement comprehensive security measures tailored to an organization's unique needs, ensuring robust protection against cyber threats.
3. Educate and Advise: Cybersecurity specialists provide guidance to individuals and organizations on best practices for safe online behavior, helping them understand how to mitigate risks effectively.
4. Respond to Incidents: In the event of a security breach, these professionals are essential in managing the response, minimizing damage, and restoring normal operations.

The rising need for cybersecurity expertise has created abundant professional opportunities. Various roles are emerging in this field, including:

- Security Analysts: Tasked with monitoring systems for suspicious activity and responding to incidents.
- Ethical Hackers: Professionals who simulate cyber attacks to identify vulnerabilities before malicious actors can exploit them.
- Compliance Specialists: Experts who ensure organizations adhere to legal and regulatory requirements regarding data protection.

As organizations recognize the value of cybersecurity, investment in training and education for professionals in this field is paramount.

Personal Data and its Privacy

With computers and internet being the integral part of life of humans in this century, the 21st century has connected the world like never before. The individuals in general and the business in particular have benefited from thegeography less environment where only the best can be purchased and only the best can be sold.

When the economies became digital the physical boundaries of markets vanished and the business became global. In initial years the internet was used for mundane jobs and to perform repetitive task. Since birth, computers and the internet itself have gone through major changes. Computers evolved from very large size machines to now being palm size. What started as a network for military operations has become World Wide Web. With these changes information isexchanged like never before.

In initial years business used this information only as data bases and was very passive in processing the information. They were mainly used for statistical purposes. But in recent times the information is being converted into data (i.e. into a format which can be used for a specific purpose) into a matter of seconds. In fact these days an individual gives away data even without his own knowledge.

An act as simple as eating at restaurants, buying goods online or even hailing ataxi gives out precious data about oneself. All the transactions that we enter into using either smart phones or the computers require individual to fill in personal data about date of birth, age sex, residential address, phone numbers and financial information. This gives away information about individual choices about what color one likes to wear, what size fits him/her, what food he/she like to eat etc. In other words an individual gives away his privacy even without his knowledge.

Businesses on the other hand are using this data for commercial purposes. The bombarding of advertisements about a product or services which you would have clicked upon while surfing through the internet hound you everywhere. Not just this there are websites, where if you have entered your date of birth and the size of dress that fits you, the website runs an algorithm by which it puts before you analysis about what your age

is, your ideal weight, if you are near or far away

from your healthy weight, what nutrition should you follow, exercise plan. It also would give you addresses of nutritionists and Gymnasiums near your area ofresidence.

Such kind of bombarding of information may not seem harmful in first instance but it definitely affects an individual's privacy. That is why economies all over the world are increasingly moving towards making laws that protect the privacy of individuals.

How is data collected

Most of the information that is collected is given away by the individual by filling forms either online or offline. It can take form of registration forms, KYC documents while you purchase, feedback forms, online surveys, downloading of various apps. Then with the help of computers vast quantity of information is processed in order to identify correlations and discover patterns in all fields of human activity.

What happens to the information that is collected?

The information is stored in vast data bases and can be mined using technology. Algorithms are being used to comb data. Enterprises around the world are using technology for its proper mining and the use of data is evolving every day. Proprietary algorithms are being developed to comb this data and analyze the trends, patterns and hidden nuances by businesses.

Many of these activities are beneficial to individuals, allowing their problems to be addressed with greater accuracy.

For instance, the analysis of very large and complex sets of data is done today through Big Data analytics. The results of this analysis can enable businesses and government to gain insights into areas such as health, transport system, farming, rural development, weather forecasts food security etc...

The reality of the digital environment today, is that almost every single activity undertaken by an individual involves some sort of data transaction or the other.

The Internet has given birth to entirely new markets:

The one dealings in the collection, organization, and processing of personal information, whether directly, or as a critical component of their business model etc Therefore, there are a large number of benefits to be gained by collecting and analyzing personal data from individuals. Pooled datasets allow quicker detection of trends and accurate targeting.

For instance, an individual‘s personal location data could be used for monitoring traffic and improving driving conditions on the road; banks can use Big Data techniques to improve fraud detection; insurers can make the process of applying for insurance easier by using valuable data from pooled data sets.

Huge data is processed by government as well. In fact state is the largest processor of data. Such personal data is used by government for such purposes as targeted delivery of social benefits, effective planning and implementation, counter terrorism operations etc.

Need to protect Personal data

Sharing data may bring benefits, the products and services are tailor made thus reducing the time and effort one spends in identifying what suits them. In today’s world often one cannot transact even simple tasks without giving away your personal information in one or the other form. But sharing of data it is not without risks. Your personal data reveals a lot about you, your thoughts, and your life. These data can easily be exploited to harm you, and that’s especially dangerous for vulnerable individuals and communities, such as journalists, activists, human rights defenders, and members of oppressed and marginalized groups.

That is why these data must be strictly protected.

When data that should be kept private gets in the wrong hands its misuse bound to

happen.

A data breach at a government agency can, for example, put top secret information in the hands of an enemy state. A breach at a corporation can put proprietary data in the hands of a competitor.

Major sources of information which are compromised and are most prone to breaches are:

1. Healthcare records
2. Criminal justice investigations and proceedings
3. Financial institutions and transactions
4. Biological traits, such as genetic material
5. Residence and geographic records
6. Social media profiles and information
7. Location-based services
8. Web surfing behavior or user preferences using persistent cookies

This all have created a need for data privacy skills which is in high demand from experts and compliance professionals. This professionals may advise the organization/business who are to comply in terms of collecting consumer data.

II. What is cyber?

The word cyber is actually a prefix often used to describe characteristic of the culture of computers, information technology and virtual reality. Having taken from Greek word "Cybernetic" meaning "governor", it became Cybernetics which means the science of communication and automatic control in both machines and living things. The term coined by Norbert Wiener (26th November 1894-18th March 1964) was an American mathematician and Philosopher who is also considered as originator of cybernetics.

What is Cyberspace?

The typical dictionary meaning of cyberspace is a notional environment in which communication over computer network occurs. In simple word it means a virtual world of internet.

What are Cyber laws?

Cyber laws deals that branch of law related to the internet. The increased in cybercrime has lead the creation of special mechanism dealing with prevention of cybercrimes that are regulated by set of cyber legislation. Therefore cyber laws are the laws governing this area.

Hence cyber law can be called as law that deals with legal issues related to use of inter-networked information technology, in short such governs the governing computers and the internet

The Internet is a global data communications system it provides connectivity between computers. The birth and rise of interest is considered to be the fourth industrial revolution also called industry 4.0. Let's take quick recap of all the industrial revolution so far:

- **1st Industrial Revolution 1765** [Period: end of 18th century till beginning of 19th century] [Industry 1.0]
  - Biggest reason mechanization
  - Agriculture replace by industry as the backbone of the societal economy
- **2nd Industrial Revolution 1870** [Industry 2.0]
  - It started at the end of the 19th century, triggered by technological advancements in the field of industries that helped the emergence of a new source of energy for instance, Electricity, gas, and oil.

- This revolution considered significant due to inventions of the automobile, and
- the plane in the beginning of the 20th century

♦ **3rd Industrial Revolution 1969** [Industry 3.0]

- Emergence of Nuclear energy
- Rise of electronics, telecommunications and of course computers
- Two major inventions, Programmable Logic Controllers (PLCs) andRobots helped give rise to an era of high-level automation

♦ **4th Industrial Revolution** 2001 [Industry 4.0]

- The birth and rise of the Internet
- Industry 4.0 is the digital transformation of manufacturing/productionand related industries and value creation processes

♦ **5th Industrial Revolution** [Industry 5.0]

- This revolution refers to people working alongside robots and smart machines
- It's about robots helping humans work better and faster by leveraging advanced technologies like the Internet of Things (Iota) and big data

III. Development of cyber legislation:

The United Nations Commission on International Trade Law (UNCITRAL) www.uncitral.org which established vide United Nations General Assembly Resolution 2205 (XXI) dated 17th December 1966. It is the core legal body of the United Nations system in the field of international trade law. In 12th June 1996 the

UNCITRAL Model Law on Electronic Commerce was adopted by UNCITRAL in1996, the additional article 5b is adopted in 1998.

- Composition:
    - Total 17 Articles, divided in two parts, where part one covers: III chapters containing 1- 15 Articles & part two: covers I chapter from Articles 16-17
    - Part one : Electronic Commerce in general
    - Part Two: Electronic commerce in specific areas
    - Article 2 contains definitions from Clause (a) to (b)
- Purpose : to enable and facilitate commerce conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability forelectronic commerce
- Significance of Model Law: legislative text to adopt the fundamental principles of non-discrimination, technological neutrality and functional equivalence that are widely regarded as the founding elements of modern electronic commercelaw
- Legislation based on or influenced by the Model Law has been adopted in 77 States and a total of 156 jurisdictions

The Information Technology Act, 2000 which is the prime legislation dealing with cyber offenses and electronic commerce in India is based on the United Nations Model Law on Electronic Commerce.

Later UNICITRAL adopted the UNCITRAL Model Law on Electronic Signatures (2001) on 5th July 2001 that objected to enable and facilitate the use of electronic

signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures.

- Brief composition:
    - Two parts:
        - Part one: Guide to Enactment of the UNCITRAL MLEScontained one chapter I: introduction to Model law
        - Part two:
            - Chapter II:
                - contains 12 articles

The Model Law on Electronic Signatures establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures as well as basic rules of conduct that may serve as guidelines for assessing duties and liabilities for thesignatory, the relying party and trusted third parties intervening in the signature process (article 6 – compliance with a requirement of signature). It also contains provisions favoring the recognition of foreign certificates and electronic signatures based on a principle of substantive equivalence that disregards the place of origin ofthe foreign signature (article 12- recognition of foreign certificates and electronic signatures). The Legislation based on or influenced by the Model Law has been adopted in 36 States

The United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005) was adopted by UNICITRAL on 23rdNovember 2005 that put into effect since 1st March 2013. It was adopted to facilitate the use of electronic communications in international trade by assuring that

contracts concluded and other communications exchanged electronically are as validand enforceable as their traditional paper-based equivalents.

- Composition:
    - Total 25 Articles
    - In IV chapters
        - I. sphere of application
        - II. General provisions
        - III. Use of electronic communication in international contracts
        - IV. Final provisions
    - Explanatory note by the UNCITRAL secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts

- Key provisions:
    - Article 1: The Convention applies to all electronic communications exchanged between parties whose places of business are in different States when at least one party has its place of business in a ContractingState
    - Article 2: Contracts concluded for personal, family or household purposes, such as those relating to family law and the law of succession, as well as

certain financial transactions, negotiable instruments, and

documents of title, are excluded from the Convention's scope ofapplication

- Article 3: it allows contractual parties to exclude its application or vary its terms within the limits allowed by otherwise applicable legislative provisions
- Article 8: it establishes the general principle that communications are not to be denied legal validity solely on the grounds that they were made in electronic form
- Article 9: It sets out criteria for establishing the functional equivalence between electronic communications and paper documents, as well as between electronic authentication methods and handwrittensignatures
- Article 10: defines the time and place of dispatch and receipt of electronic communications, tailoring the traditional rules for these legal concepts to suit the electronic context and innovating with respect to the provisions of the Model Law on Electronic Commerce
- Article 11: The Convention further clarifies that a proposal to conclude a contract made through electronic means and not addressed to specific parties amounts to an invitation to deal, rather than an offer whose acceptance binds the offering party, in line with the corresponding provision of the CISG
- Article 12 : with respect to the proliferation of automated message systems, the Convention allows for the enforceability of contracts entered into by such systems, including when no natural person reviewed the individual actions carried out by them

- Article 14 : It establishes remedies in case of input errors by natural persons entering information into automated message systems

IV. The Information Technology Act, 2000 (hereafter IT Act, 2000)

The IT Act, 2000 is the legislation that regulated the computer, computer system, computer network and information in electronic format. According to the preamble the act meant to provide legal recognition to electronic transaction meaning transactions carried out through electronic communication also referred as E-commerce that includes everything which is alternative to paper based communication for instance, email, messages through electronic platforms etc.

The act has spread over to 13 chapters and 90 sections [Sections 91, 92, 93 and 94of the principal Act were omitted by the Information Technology (Amendment) Act 2008] and has 2 Schedules [Schedules III and IV were omitted by the IT (Amendment) Act, 2008]

- Brief Composition :

1. Chapter – I – Preliminary (sections 1 & 2)
2. Chapter – II – Digital Signature and Electronic Signature (Sections 3 &3A)
3. Chapter – III – Electronic Governance (Sections 4 to 10A)
4. Chapter – IV – Attribution, Acknowledgement and Dispatch of Electronic Records (Sections 11 to 13)
5. Chapter – V – Secure electronic records and secure electronic signatures (Sections 14 to 16)
6. Chapter – VI – Regulation of Certifying Authorities (Sections 17 to 34)
7. Chapter – VII – Electronic Signature Certificates (Sections 35 to 39)
8. Chapter – VIII – Duties of Subscribers (Sections 40 to 42)
9. Chapter – IX – Penalties, Compensation and Adjudication (Sections 43 to47)
10. Chapter X – The Appellate Tribunal (Sections 48 to 64)
11. Chapter XI – Offences (Sections 65 to 78)
12. Chapter XII – Intermediaries not to be liable in certain cases (Section 79)
13. Chapter XIIA – Examiner of Electronic Evidence (Section 79A)
14. Chapter XIII – Miscellaneous (Sections 80 to 90)

What is Digital and Electronic signature?

The Digital Signature is defined under Section 2 (P) of the act. The definition is reiterated below

"**Digital signature"** means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

Further the Section 2 (q) defines "**Digital Signature Certificate"** as a Digital Signature Certificate issued under sub-section (4) of section 35;

Likewise the Section 2 (ta) of the act defines electronic signature and the same is reiterated below

"**Electronic Signature**" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature;

Further the Section 2 (tb) of the act defines **Electronic Signature Certificate** means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate;]

The term electronic signature was added via amendment in 2008 act, it is broader than digital signature.

According to the **UNCITRAL,** electronic authentication and signature methods may be classified into the following categories –

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those bases on the physical features of the user, i.e., biometrics.
- Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.

- Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

According to the UNCITRAL MODEL LAW on Electronic Signatures, the following technologies are presently in use –

- Digital Signature within a public key infrastructure (PKI)
- Biometric Device
- PINs
- Passwords
- Scanned handwritten signature
- Signature by Digital Pen
- Clickable "OK" or "I Accept" or "I Agree" click boxes

It should be noted that the IT Act, 2000 has amended in year 2002, 2008 and2017.

1. **The Negotiable Instruments (Amendment and Miscellaneous Provisions) Act, 2002** effective from 26th Feb 2003:
    - Insertion of section 81A in the IT Act 2000
    - "application of the act to electronic cheque and truncated cheque"
    - Section 6 (a) of the Negotiable Instrument Act,1881 "a cheque in the electronic form" means a cheque drawn in electronic form by using any

computer resource and signed in a secure system with digital signature (with or without biometrics signature) and asymmetric crypto system or with electronic signature, as the case may be;

- Section 6 (b) of the Negotiable Instrument Act, 1881 : (b) "a truncated cheque" means a cheque which is truncated during the course of a clearing cycle, either by the clearing house or by the bank whether paying or receiving payment, immediately on generation of an electronic image for transmission, substituting the further physical movement of the cheque in writing

2. **The IT (Amendment) Act, 2008** effective from 27th October 2009:

- Introducing Digital Signatures: With the passage of the IT (Amendment) Act, 2008 India has become technologically neutral due to adoption of electronic signatures as a legally valid mode of executing signatures.
- Introducing Corporate Responsibility (Sec. 43A): Corporate bodies handling sensitive personal information or data in a computer resource are under an obligation to ensure adoption of 'reasonable security practices' to maintain its secrecy, failing which they may be liable to pay damages/compensation.

- Analysis of the Amended Sec. 43: The amended Act provides the distinction between 'contravention' and 'offence' (section 43 for contraventions and section 66 of the Act for offences). As per the Amendment Act, 2008, there is no ceiling limit for compensation under section 43 which was one crore rupees in the IT Act.
- New Definitions Added: Two very important definitions are added to the IT Act through IT Amendment Act,2008- Section 2(ha)-"Communication device " and Section 2 (w)
  –"intermediary".
- Emphasizing the legality of electronic documents: Newly added sections 7A and 10A in the amended Act reinforce the equivalence of paper based documents to electronic documents.
- Update on the Power of Controller: The role of the Controller to act as repository of digital signatures has been repealed by the IT Amendment Act, 2008. This role has now been assigned to the Certifying Authority in Section 30 of the IT Act.The power of Controller to intercept information being transmitted through a computer resource, when necessary, in national interest is amended in Section 69.

- Update on the role of Adjudicating Officer: As per the Section 46 in the amended ACT the Adjudicating officers have been conferred with powers of execution of orders passed by it, including order of attachment and sale of property, arrest and detention of accused and appointment of receiver. This empowers theoffice of adjudicating officer and extends greater enforceability and effectiveness of its orders.
- Changes in Cyber Appellate Tribunal: As per section 52 D, the tribunal would now consist of Chairperson and other members as appointed by the Central Government and their decision- making power.
- New Addition to the list of Cybercrimes: Section 66 in the amended Act lists all the new cybercrimes for which no provisions existed in the IT Act, 2000.
- Update on Cyber crime prosecution: Section 67 talks about conviction for imprisonment for a term not exceeding 2 yrs or fine not exceeding one lac or both for not preserving information.
- Blocking unlawful websites: Section 69A has been inserted in the IT amendments 2008 and gives power to Central government or any authorized

officer to direct any agency or intermediary(forreasons recorded in writing) to block websites in special circumstances as applicable in Section 69 and its punishable offences.

- Monitor of data traffic: Section 69 B confers onthe Central government power to appoint any agency to monitor and collect traffic data or information, failing to extend cooperation in this respect is punishable offence.
- Defining "Critical Information Infrastructure": The newly added Section 70 in the Amendment Act 2008 defines what is "critical information infrastructure" and encompasses the protection of information is equally important as is the maintaining of security and sovereignty of India.
- Section 77, 78 and 80 in the amended ACT talks about conferring power to investigate offences under the Act from DSP level to Inspector level which will be instrumental in quicker investigationin the cybercrime cases provided adequate tools and training is provided.
- Liability of the intermediary modified: The amended Section 79 states that the intermediary shall not be liable for any third-party information

if it is only providing access to a communication system.

- Electronic Evidence Examiner: With amendments in 2008, Section 79 A is added that empowers the Central government to appoint any department or agency of Central or State government as Examiner of Electronic Evidence.
- Penalty And Compensation for the Damage to Computer, System and other related devices

3. **The Finance Act, 2017** effective from 26th may 2017**:**

- Vide Section 169 of the Finance Act, 2017 the cyber appellate tribunal replaced with the Telecom Disputes Settlement and Appellate Tribunal
- **sections 49, 50, 51, 52, 52A, 52B, 52C, 53, 54 and 56** were omitted

The definition have contained under section 2 (1) (a) to (zh) of the act, some of the relevant definitions have explained under:

1. Certifying authority: Section 2 (1) (g) defines that a person who has been granted a license to issue a [Electronic Signature] Certificate under Section 24;

Under section 24 the controller after receiving the appropriate application and along with doctors will have to certify grant the

License or reject the application. Therefore such controller is to be defined as the certifying authority under the act. Here the "Controller" means the Controller of Certifying Authorities

2. Data : section 2 (1) (o) defines "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
3. Electronic record : Section 2 (1) (t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;
4. section 2 (1) (za) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;
5. section 2 (1) (zg) "subscriber" means a person in whose name the [Electronic Signature] Certificate is issued;

It should be noted that legal recognition to electronic records by virtue of section 4 is been provided the section reads as under:

"Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference

Similarly for electronic signatures:

"Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of [electronic signature] affixed in such manner as may be prescribed by the Central Government".

Use of electronic records and [electronic signatures] in Government and its agencies

Section 6 of the IT act states that if any law requires / provides for

(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner

(b) the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner, then such can be effected by electronic form

Penal provision under the IT Act, 2000

The penalty provision have provided under Chapter XI of the act covering ss 65 to78.

1. Section 65. Tampering with computer source documents.
2. Section 66. Computer related offences.
3. Section 66A. Punishment for sending offensive messages through communication service, etc.
4. Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device.
5. Section 66C. Punishment for identity theft.
6. Section 66D. Punishment for cheating by personation by using computer resource.
7. Section 66E. Punishment for violation of privacy.
8. Section 66F. Punishment for cyber terrorism.
9. Section 67. Punishment for publishing or transmitting obscene material in electronic form.
10. Section 67A. Punishment for publishing or transmitting of materialcontaining sexually explicit act, etc., in electronic form.
11. Section 67B. Punishment for publishing or transmitting of materialdepicting children in sexually explicit act, etc., in electronic form.
12. Section 67C. Preservation and retention of information by intermediaries.
13. Section 68. Power of Controller to give directions.
14. Section 69. Power to issue directions for interception or monitoring ordecryption of any information through any computer resource.

15. Section 69A. Power to issue directions for blocking for public access of any information through any computer resource.
16. Section 69B. Power to authorize to monitor and collect traffic data orinformation through any computer resource for cyber security.
17. Section 70. Protected system.
18. Section 70A. National nodal agency.
19. Section 70B. Indian Computer Emergency Response Team to serve asnational agency for incident response.
20. Section 71. Penalty for misrepresentation.
21. Section 72. Penalty for Breach of confidentiality and privacy.
22. Section 72A. Punishment for disclosure of information in breach of lawful contract.
23. Section 73. Penalty for publishing electronic signature Certificate false in certain particulars.
24. Section 74. Publication for fraudulent purpose.
25. Section 75. Act to apply for offence or contravention committed outsideIndia. 76. Confiscation
26. Section 77. Compensation, penalties or confiscation not to interfere withother punishment
27. Section 77A. Compounding of offences
28. Section 77B. Offences with three years imprisonment to be bailable
29. Section 78. Power to investigate offences

V. Below is list of Rules and Regulations under the Information Technology Act, 2000

1. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 enacted vide sub section (1), clause (z) & (zg) of sub section (2) of section 87 of the IT Act, 2000
2. The Information Technology (Intermediary Guidelines) Rules, 2011 enacted vide clause (zg) of sub section (2) of section 87 r. w. sub section (2) of section 79 of the IT Act, 2000

3. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 enacted vide clause (ob) of sub section (2) of section 87 r. w. section 43A of the IT Act, 2000
4. The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Clause (z) of sub section (2) of section 87, r. w. sub section (2) of section 69A of the IT Act, 2000
5. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 enacted vide Clause (y) of sub section (2) of section 87 r. w. sub section (2) of section 69 of the IT Act, 2000
6. The Information Technology (Guidelines for Cyber Café) Rules, 2011 enacted vide clause (zg) of sub section (2) of section 87 r. w. sub section (2) of section 79 of the IT Act, 2000
7. The Information Technology (Electronic Service Delivery) Rules, 2011 enacted vide clause (ca) of sub section (2) of section 87 r. w. sub section 6A of the Information Technology Act, 2000
8. The Information Technology (Qualification And Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 enacted vide clauses (p) and (q) of sub section (2) of section 87 of the IT Act, 2000
9. The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 enacted vide clause (zf) of sub section (2) of section 87 r. w. sub section (5) of section 70B of the IT Act, 2000

Regulations under the IT Act, 2000

10. The Information Technology (Certifying Authorities) Regulations, 2001 enacted vide section 89 of the IT Act, 2000
11. The Information Technology (Recognition of Foreign Certifying Authorities operating under a Regulatory Authority) Regulations, 2013 enacted vide clause (a) of sub section (2) of section 89 of the IT Act, 2000

Following the 2008 Amendment, the government notified the following four Rules on April 11, 2011.

1. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, prescribe security standards for personal information stored electronically
2. The IT (Intermediary Guidelines) Rules, 2011, provide due diligence requirements for intermediaries.
3. The IT (Guidelines for Cyber Café) Rules, 2011, require cyber cafés to identify users and maintain records of use.
4. The IT (Electronic Service Delivery) Rules, 2011, provide a framework for electronic delivery of services such as licenses, forms and certificates.

VI. GENERAL DATA PROTECTION REGULATION

The European Union's GDPR designed to "harmonise" data privacy laws across all of its member's countries as well as providing greater protection and rights to individuals. GDPR was also created to alter how businesses and other organisations can handle the information of those that interact with them. There's the potential for large fines and reputational damage for those found in breach of the rules.

The regulation has introduced big changes but builds on previous data protection principles. As a result, it has led to many people in the data protection world, including UK information commissioner Elizabeth Denham, to

liken GDPR to an evolution, rather than a complete overhaul of rights. For businesses which were already complying with pre-GDPR rules the regulation should have been a "step change," Denham has said.

Despite a pre-GDPR transition period taking place, which allowed businesses and organisations time to change their policies, there has still been plenty of confusion around the rules. Here's our guide to what GDPR really means.

What is GDPR exactly?

GDPR can be considered as the world's strongest set of data protection rules, which enhance how people can access information about them and places limits on what organisations can do with personal data. The GDPR contains 99 individual articles.

The regulation exists as a framework for laws across the continent and replaced the previous 1995 data protection directive. The GDPR's final form came about after more than four years of discussion and negotiations – it was adopted byboth the European Parliament and European Council in April 2016. The underpinning regulation and directive were published at the end of that month.

GDPR came into force on May 25, 2018. Countries within Europe were given the ability to make their own small changes to suit their own needs. Within the UK this flexibility led to the creation of the Data Protection Act (2018), which superseded the previous 1998 Data Protection Act.

Personal data means any data identified and identifiable natural person. The regulation lays down fundamental norms to protect the privacy of personal data.

Consisting of total ninety nine articles covered in X chapters the regulation provide a comprehensive set of provision applicable to all European residents.

Brief composition of EU GDPR 2016 for understanding:

Chapter	**Articles**	**Provision**
I. General Provision	1-4	1. Subject matter and objectives

		2. Material scope
		3. Territorial scope
		4. Definitions
II. Principles	5-11	5. Principles relatingto processing personal data
		6. Lawfulness of processing
		7. Conditions of consent
		8. Conditions applicable to child's consent in relation to information society services
		9. Processing of special categories of personal data
		10.Processing of personal data relating to criminal convictions and offences
III. Rights of the data subject	Section 1-5	**Sections** 1. Transparency and modalities

		2. Information and access to personal data
		3. Rectification and erasure
		4. Right to object and automated individual decision making

		5. Restrictions
IV. Controller and Processor	Section 1-5	**Sections** 1. General obligations
		2. Security of personal data
		3. Data protectionimpact assessmentand prior consultation
		4. Data protection officer
		5. Codes of conduct and certification
V. Transfers of personal data to third countries or international organisations	Article 44-50	44. general principles for transfer
		45. transfers on the basis of an adequacy decision
		46. transfers subject to appropriate safeguards
		47. binding corporate rules
		48. transfers or disclosures not authorised by union law
		49. derogations for specific situations

		50. international cooperation for the protection of personal data
VI. Independent supervisory authorities	Section 1-2	**Sections** 1. Independent status
		2. Competence, tasks and powers
VII. Cooperation	Section 1-3	**Sections**

	and consistency		1. Cooperation
			2. Consistency
			3. European data protection board
VIII.	Remedies, liability and penalties	Article 77-84	77. right to lodge a complaint with supervisory authority
			78. right to an effective judicial remedy against a supervisory authority
			79. right to an effective judicial remedy against a controller or processor
			80. representation of data subjects
			81. suspension of proceedings
			82. right to compensation and liability
			83. general conditions for imposing administrative fines
			84. penalties
IX.	Provisions relating to specific processing situations	Article 85-91	85. processing and freedom of expression and information
			86. processing and public access to official documents

		87. procession of national identification number
		88. processing in the context of employment
		89. safeguards and derogations relating to processing for archiving purposes in the public

		interest, scientific or historical research purposes or statistical purposes
		90. obligation of secrecy
		91. existing data protection rules of churches and religious associations
X. Delegated acts and implementing acts	Article 92-93	92. exercise of delegation
		93. committee procedure
XI. Final provisions	Article 94-99	94. Repeal of directive 95/46EC
		95. relationship with directive 2002/58/EC
		96. relationship with previously concluded agreements
		97. commission reports
		98. review of other union legal acts on data protection
		99. entry into force and application

VII. The Personal Data Protection Bill, 2019

Interestingly recognizing the importance of data protection our country too has taken positive step in the form of **Personal Data Protection Bill, 2019** that introduced in Loksabha on 11th December 2019. Although the enactment of the same is still on hold it incorporate crucial features of GDPR.

Key takeaway from bill's provision

Purpose: Provides for protection of personal data of individuals, and establishes aData Protection Authority for the same

Composition of bill:

1. Total chapters : XIV
2. Total sections : 98
3. Total schedule : one
4. Total definition : Section 3 (1) to (40) = 40 definitions

- The Bill provides a framework for safeguarding the privacy of personal data of individuals (dataprincipals) which is processed by entities (data fiduciaries)
- The Bill sets up a national-level Data Protection Authority (DPA) to supervise and regulate data fiduciaries.

  The Authority may:

  (i) take steps to protect interests of individuals,

  (ii) prevent misuse of personal data, and

(iii) Ensure compliance with the Act.

- It will consist of a chairperson and six members, with at least 10 years' expertise in the field of data Protection, information technology or public administration.
- **The Bill governs the processing of**
- Personal data by:

  (i) government,

  (ii) companies incorporated in India, and

  (iii) Foreign companies dealing with personal data of individuals in India.
- The Bill categorizes certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator
- **Personal data** is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual.
- The Bill classifies certain categories of personaldata as

  1. **Sensitive personal data**: This includes financial data, biometric data, caste, religious or

political beliefs, or any other category of data as specified.

2. **data fiduciary** as the entity or individual who decides the means and purpose of processing personal data, and data principal as the individual to whom the data relates

In the landmark case of Justice K.S. Puttuswamy v. Union of India , (2017) 10 SCC 641. The apex court held that the privacy being a fundamental right flows fromthe right to life and personal liberty under Article 21 of the Constitution. The Court also observed that privacy of personal data and facts is an essential aspect of the right to privacy. In July 2017, a Committee of Experts, chaired by Justice B.

N. Srikrishna, was set up to examine various issues related to data protection in India. The committee submitted its report titled "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians" along with draft in July 2018 to the M/o Electronic and Information Technology.

The personal data protection bill, 2019 is pending with the Joint parliamentary committee since March 2020 , that has granted fifth extension so far. It is likely to be submitted in the upcoming winter session 2021 of parliament.

Presently the usage and transfer of personal data of citizens is regulated by the IT Rules 2011. It holds the companies using the data liable for compensating the individual, in case of any negligence in maintaining security standards while dealing with the data.

Non-Personal Data

The Non-personal data as the name suggest is exactly as oppose to Personal data in other words a data without personally identifiable information.

To put it simply the non personal data can be identified as a data which was neverrelated to natural person. Currently as under the Personal Date Protection Bill, 2019, the government is empowered to direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data toenable better targeting of delivery of services or formulation of evidence-based policies by the Central Government (subsection (2) of Section 91).

In an attempt to study issues relating to the non-personal data the nodal ministry of electronics and information technology formed a expert committee in around July 2020.

Observation of committee:

The non-personal data should be regulated to

(i) Enable a data-sharing framework to tap the economic, social, and publicvalue of such data, and
(ii) Address concerns of harm arising from the use of such data.

Non-personal data authority: It will be establish for putting in place the framework for the governance of non-personal data. The authority shall be entrusted with framing of guidelines with reference to data sharing and riskassociated with non-personal data

PERSONAL DATA PROTECTION APPROACHES WORLDWIDE

Realizing the need to protect data governments all over the world have taken measures to protect it. The government is entrusted with the task of protecting the business and allowing them freedom to do business and at the same time to ensure that privacy of individual is protected.

The Right to privacy stems from the constitutions in some countries e.g. EuropeanUnion and India while it is ensured by various legislations in countries like United States of America, Australia and china. For these reasons there have been different approaches around the world while dealing with Personal dataprotection regulations.

European Union:

In case of European Union the need for protection of personal data stems from the Right to Respect and personal Dignity. Right to dignity is ensured throughright to privacy. The European Union enacted the General Data protection Regulation (GDPR) which all the member countries follow. The bases of right to privacy is how an individual can control over one's public image. The EU regulations give right to self –determination i.e. the ability to control the information that is disclosed about ourselves. It also ensures that personal data that is collected can be corrected and should be deleted with ease. An individual has to give consent to his/ her data being processed, and it should be equally easyto withdraw such consent.

Most of the countries in the world are affected by GDPR and have begun to comply with these regulations because it applied to all the companies around the world who process data of citizens of European Union.

Below is the list of legislations enacted in different countries which are on similar footing that of GDPR

Sr. no.	Name of the country	Legislation
1	Bahrain	Personal data protection law, 2019
2	Israel	Data security regulations, 2017
3	Qatar	
4	Turkey	Law on protection of personal data no. 6698 enacted in 2016
5	Kenya	Data protection act, 2019
6	Mauritius	Data protection act, 2017

7	Nigeria	Data protection regulation, 2019
8	South Africa	Protection of personal information (POP) act, 2020
9	Uganda	Data protection and privacy

		act, 2019
10	Japan	Act on the protection of personal information (APPI), 2020
11	New Zealand	Privacy act, 2020
12	South Korea	Personal information protection act, 2011
13	Argentina	Personal data protection act, 2001
14	Brazil	General data protection law, 2020
15	Uruguay	Act on the protection of personal data and habeas data action, 2008
16	Canada	Personal information protection and electronic documents act, 2000

The United States of America

The core of privacy with Americans is the "Sanctuary of home". The USA follows a Lizze Faire approach i.e. minimalistic interference from government. There is no single law to protect privacy of the US citizens. However the protection is ensured by enacting specific laws over specific subjects.

There is no specific Authority for data protection but federal trade commission ensures that the companies do not engage in unfair and deceptive trade practices.

China

China’s perspective on personal data protection has been primarily been from the perspective of averting National security risks. It protects the privacy of its citizens by enforcing strict regulations over cross-border transfer of data.

Australia and Singapore

Privacy is not a fundamental right in these countries. Also both these countries do not bring government under the purview of data protection. Singapore in fact is very business friendly country and projects its self to be the global data processing destination.

India

The Indian constitution works on two planks one it states that "state" is facilitator of human progress and second that state is prone to excess. Hence it is checked by effectuating by vertical and horizontal separation of powers. Also the constitution of India grants every individual fundamental right which it can exercise against the state.

Right to privacy had not been recognized as fundamental right until the Supreme Court gave its decision in Justice K.S. Puttaswamy (Retd.) v. Union of India. The article 21 of the constitution states that "No person shall be deprived of his life or personal liberty except according to the procedure given by law. It means that even the state while exercising its right has to follow certain procedure as laid down by law. Right to privacy stems from right to personal liberty. Liberty of every citizen within the frame of being lawful and constitutional

Hence India has followed an approach of being facilitator to businesses and at the same time protecting the rights of its citizens.

The challenge for regulators is to frame mechanisms wherein it is possible to utilize data while simultaneously protecting an individual's privacy preferences and their personally identifiable information. Hence, the laws and regulations related to Privacy and Data Protection are constantly changing, as lawmakers endeavor strict and diligent compliance with data privacy and security regulations.

The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Act)

The Aadhaar Act enables the Government to collect identity information from citizens including their biometrics, issue a unique identification number or an Aadhaar Number

on the basis of such biometric information132, and thereafter provide targeted delivery of subsidies, benefits and services to them.

The requesting entity (government/public and private entities/agencies) is required to obtain the consent of the individual before obtaining her identity information for the purpose of authentication and must use her identity information only for the purpose of authentication.

Data protection norms for personal information collected under the Aadhaar Act are also found in The Aadhaar (Data Security) Regulations, 2016 (Aadhaar Security Regulations). The Aadhaar Security Regulations impose an obligation on the UIDAI to have a security policy which sets out the technical and organizational measures which will be adopted by it to keep information secure.

Financial Sector

The primary legislations that address data protection in financial sector are the Credit Information Companies (Regulation) Act, 2005 (CIC Act), the Credit Information Companies Regulation, 2006 (CIC Regulations)

- **The CIC Act** primarily applies to credit information companies (CICs) and recognises them as collectors of information.
- The CIC Act imposes an obligation on CICs to adhere to privacy principles at the stage of collection, use and disclosure of credit information, and requires them to ensure that credit information held by them is accurate, complete and protected against loss or unauthorized use, access and spdisclosure.
- **The CIC Regulations** impose an obligation on CICs to ensure data security and secrecy. It also requires them to adhere to a large number of recognized data protection principles such as: data collection limitation, data use limitation, data accuracy, data retention and access and modification

Telecom Sector

There are multiple laws that operate in the telecom sector such as the Indian Telegraph Act, 1885 (Telegraph Act), the Indian Wireless Telegraphy Act, 1933, the Telecom

Regulatory Authority of India Act, 1997 (TRAI Act) and various regulations issued there under.

- Data protection norms in the telecom sector are primarily dictated by the Unified License Agreement (ULA) issued to Telecom Service Providers (TSP) by the Department of Telecommunications (DoT).
- The DoT has prescribed the format in which, and the types of information that are to be collected from the individual.
- A TSP has an obligation to take necessary steps to safeguard the privacy and confidentiality of the information of individuals to whom it provides a service and from whom it has acquired such information by the virtue of the service provided.

Health Sector

- The Clinical Establishments (Central Government) Rules, 2012 (Clinical Establishments Rules) requires clinical establishments to maintain and provide Electronic Medical Records/Electronic Health Records, thus mandating the storage of health information in an electronic format.
- The SPDI Rules recognize health information as constituting "sensitive personal data "and thus regulates its collection, use and disclosure.
- However, as already mentioned the SPDI Rules apply only to the private sector thus leaving the whole of the public health sector outside its ambit.

SPECIMEN PRIVACY POLICY

1. Introduction

Begin with a brief general statement on:

- why privacy matters to you

- the information contained within the privacy notice (i.e. clear and concise summary)
- what services the notice applies to (e.g. website, software, purchases, subscription, etc)
- You may include an encouragement for the user to read the policy carefully and contact you with any questions or concerns about your privacy practices.

2. Who we are?

Provide name and contact details of the data controller. This will typically be your business or you, if you are a sole trader. Where applicable, you should include theidentity and contact details of the controller's representative and/or the data protection officer.

3. What information do we collect?

Specify the types of personal information you collect, e.g. names, addresses, user names, etc. You should include specific details on:

- how you collect data (e.g. when a user registers, purchases or uses your services, completes a contact form, signs up to a newsletter, etc)
- what specific data you collect through each of the data collection method
- if you collect data from third parties, you must specify categories of data and source
- If you process sensitive personal data or financial information, and how you handle this you may want to provide the user with relevant definitions in relation to personal data and sensitive personal data.

4. How do we use personal information?

Describe in detail all the service- and business-related purposes for which you will process data.

For example, this may include things like:

- personalization of content, business information or user experience
- account set up and administration
- delivering marketing and events communication
- carrying out polls and surveys
- internal research and development purposes
- providing goods and services

- legal obligations (e.g. prevention of fraud)
- meeting internal audit requirements

Please note this list is not exhaustive. You will need to record all purposes for which you process personal data.

5. What legal basis do we have for processing your personal data?

Describe the relevant processing conditions contained within the law. There are six possible legal grounds:

- Consent
- Contract
- Legitimate interests
- Vital interests
- Public task
- Legal obligation

Provide detailed information on all grounds that apply to your processing, and why. If you rely on consent, explain how individuals can withdraw and manage their consent. If you rely on legitimate interests, explain clearly what these are.

If you're processing special category personal data, you will have to satisfy at leastone of the six processing conditions, as well as additional requirements for processing under the GDPR. Provide information on all additional grounds that apply.

6. When do we share personal data?

Explain that you will treat personal data confidentially and describe the

circumstances when you might disclose or share it. E.g, when necessary to provide your services or conduct your business operations, as outlined in your purposes for processing. You should provide information on:

- How you will share the data
- What safeguards you will have in place
- What parties you may share the data with and why

7. Where do we store and process personal data?

If applicable, explain if you intend to store and process data outside of the data subject's home country. Outline the steps you will take to ensure the data is processed according to your privacy policy and the applicable law of the country where data is located. If you transfer data outside the country, outline the measures you will put in place to provide an appropriate level of data privacy protection. E.g. contractual clauses, data transfer agreements, etc.

8. How do we secure personal data?

Describe your approach to data security and the technologies and procedures you use to protect personal information. For example, these may be measures:

- To protect data against accidental loss
- To prevent unauthorized access, use, destruction or disclosure
- To ensure business continuity and disaster recovery
- To restrict access to personal information
- To conduct privacy impact assessments in accordance with the law and your Business policies
- To train staff and contractors on data security
- To manage third party risks, through use of contracts and security reviews

Please note this list is not exhaustive. You should record all mechanisms you rely on to protect personal data. You should also state if your organization adheres to certain accepted standards or regulatory requirements.

9. How long do we keep your personal data for?

Provide specific information on the length of time you will keep the information for in relation to each processing purpose. The GDPR requires you to retain data for no longer than reasonably necessary. Include details of your data or records retention schedules, or link to additional resources where these are published.

If you cannot state a specific period, you need to set out the criteria you will apply to determine how long to keep the data for (e.g. local laws, contractual obligations, etc) you should also outline how you securely dispose of data after you no longer need it.

10. Your rights in relation to personal data

Under the GDPR, you must respect the right of data subjects to access and control their personal data. In your privacy notice, you must outline their rights in respectof:

- Access to personal information
- Correction and deletion
- Withdrawal of consent (if processing data on condition of consent)
- Data portability
- Restriction of processing and objection
- lodging a complaint with the Information Commissioner's Office

You should explain how individuals can exercise their rights, and how you plan to respond to subject data requests. State if any relevant exemptions may apply and set out any identity verifications procedures you may rely on. Include details of the circumstances where data subject rights may be limited, e.g. if fulfilling the data subject request may expose personal data about another person, or if you're asked to delete data which you are required to keep by law.

11. Use of automated decision-making and profiling

Where you use profiling or other automated decision-making, you must disclose this in your privacy policy. In such cases, you must provide details on existence of any automated decision-making, together with information about the logic involved, and the likely significance and consequences of the processing of the individual.

12. How to contact us?

Explain how data subject can get in touch if they have questions or concerns about your privacy practices, their personal information, or if they wish to file a complaint. Describe all ways in which they can contact you – e.g. online, by email or postal mail.

If applicable, you may also include information on:

13. Use of cookies and other technologies

You may include a link to further information, or describe within the policy if you intend to set and use cookies, tracking and similar technologies to store and manage user preferences on your website, advertise, enable content or otherwise analyze user and usage data. Provide information on what types of cookies and technologies you use, why you use them and how an individual can control and manage them.

14. Linking to other websites / third party content

If you link to external sites and resources from your website, be specific on whether this constitutes endorsement, and if you take any responsibility for the content (or information contained within) any linked website.

You may wish to consider adding other optional clauses to your privacy policy, depending on your business' circumstances.

Conclusion:

It is said that nothing is permanent except Change. And one who rides the wave of change survives. This is the theory of Survival of the Fittest. The evolution emphases that

change are inevitable. It laid out that for anyone to survive

adopting the change was the only means of survival. Incorporating a change makes you equipped to fight challenges of survival. This theory holds true for our profession too. The more we adapt to the new environment, learn new technology, understand new laws and procedures, the more we evolve to be fittest to survive.

Lastly I would like to conclude that every change brings opportunity, which will help us break through the traditional roles. With the opportunities in Cyber space, we can transcend into global markets with our immense knowledge.

Let us march towards better horizons with confidence and utmost faith in ourselves.

Quick links to refer:

1. m/o electronics and information technology https://www.meity.gov.in/
2. department of administrative reforms and public grievance https://pgportal.gov.in/
3. open government data platform india https://data.gov.in/
4. government of India https://www.mygov.in/
5. biometric attendance system https://attendance.gov.in/
6. e-governance standards http://egovstandards.gov.in/
7. a national e-authentication service https://epramaan.gov.in/
8. PHD scheme for electronics and IT https://phd.dic.gov.in/
9. Invest India https://www.investindia.gov.in/
10. The national mobile governance initiative https://mgov.gov.in/
11. Digi locker https://www.digilocker.gov.in/dashboard
12. national voters service portal https://www.nvsp.in/
13. Indian computer emergency response team https://cert-in.org.in/
14. Digital India Corporation https://dic.gov.in/
15. National informatics centers services https://nicsi.com/
16. National internet exchange of India https://nixi.in/
17. Center for development of advance computing https://www.cdac.in/
18. Center for material of electronics technology https://cmet.gov.in/
19. Education and research in computer networking https://ernet.in/
20. National institute of electronics and information technology https://www.nielit.gov.in/
21. SAMEER www.sameer.gov.in
22. Software technology parks on India https://stpi.in/home
23. Unique Identification Authority of India https://uidai.gov.in/
24. UNCITRAL https://uncitral.un.org/

25.COMPLIANCE TO EU GDPR https://gdpr.eu/