



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

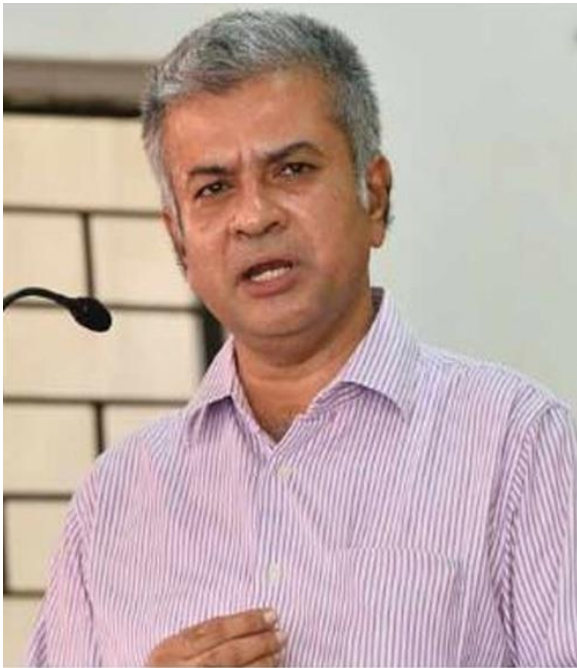
DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK
LEGAL

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and diploma in Public

a professional Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



Senior Editor

Dr. Neha Mishra



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Utranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.



Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US



WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

W H I T E B L A C K
L E G A L

SIGNIFICANCE OF DATA PROTECTION STANDARDS IN PROTECTING PRIVACY RIGHTS OF EMPLOYEE

AUTHORED BY - VIDYA M.N

INTRODUCTION:

The current work gives an overview of legal standards related to employee's personal data protection and privacy. The paper explores the recent trends, various global principles and good practices in nexus with domain of working environment. The aim is to give a regional and global approach in the interest of contemporary view on the leading basic legal principles and standards in this filed. The paper exposes to application of general data protection principles in the context of employment relationship and new technological evolutions.¹

The structure of the research paper includes introduction with the brief idea of the data protection and its standards and its legal evolution. The specific paper deals with regional and global data protection standards with the general perspective as well as employment specific perspective.

The development in the arena of personal data protection has strongly evolved in recent years. Many world countries have led to enforcement of data protection laws. ILO in the early days adopted Code of Practice on the protection of worker's personal data and recently European Union came-up with the robust law, the 'General Data Protection Regulation (GDPR)' in 2018. The new era of data protection has rejuvenated, as a result more than 130 countries holds its own data protection principles now.

With reference to the understanding of Privacy and Data protection priorly, the personal data protection needs to broader approach of right to privacy. The privacy and data protection are interdependent and overlapping legal concepts. It is been accepted the right to data protection

¹ **Hendrickx Frank, "Protection of Workers' Personal Data: General Principles" *International Labour Organization Working Papers.* [available at <https://webapps.ilo.org/static/english/intserv/working-papers/wp062/index.html>]**

is a part of right to privacy.² The privacy is a notion which emphasizes the personal data protection. Way back the concept 'privacy' was defined as 'the right to be let alone'. Since then, the protection of privacy has evolved strongly with a broader coverage of private life as well as public life of an individual. The notion of privacy has become more flexible, interpretative and responsive and adaptive to the newer settings (which includes data protection of workers in the world of work).

Another understanding is both these notions are connected to social, economic and political rights, where the right to privacy is accepted universally as a human right. Hence, the data protection principles need to be understood with common baseline in account of different jurisdictional approaches at international level.

In the specific context of employment relationship, the workers have a right to privacy based on international and regional human rights regimes. The principle of data protection and right to privacy are guaranteed for all workers regardless of type of employment or contractual agreements or employment status. Adding to this, the rights of workers are not only protected with respect to employers, but also by the other parties, such as co-workers, worker's organisation, government and so on.

It is apparent that the recent technological challenges and new evolutions such as digitization, big data, internet of things, artificial intelligence and robotisation has affected the work environment, as a result much attention is given to privacy and data protection rights in an increased pace. The electronic and computer data has been considered more significant. The dynamic nature of privacy has adopted over time as privacy 4.0 in response to industry 4.0. Numerous regulations started to adopt the rules to address the issues of privacy and data protection. Now the world is concerned about unlimited data processing, the interconnected centralised data, free and fast flow of data, asymmetrical information, unnecessary disclosure of information, manipulation of data and so on. As a futuristic approach the countries should have a dynamic law where it is ready to adopt any technological encounters.

Another critical dimension of data protection law relevant to the era of privatization has literally changed the work culture which paved the way for new ways of working where difference between the sphere of work and private life is vague. Through the introduction of digital workplace and online communication, the employees have mixed the private and professional communication by utilising the professional communication systems for personal

² The case of European Human Rights Court is a best example where the rules of data protection is conceived under the concept of right to privacy. Another example is, in South Africa the right to personal data protection is considered as derivative of Constitutional Right to privacy, similar to Indian approach.

reasons and visa-versa, which made difficult to monitor the data of employees. On the other hand, new arena of employment relationship has adopted which facilitated the worker to work on flexible time without boundary management. Further, the emergence of social media has impacted the relationship of employment by creating additional tensions.

The concept of 'Privacy' has not been addressed in any Indian Legislation. When there is a need to interpret the meaning of the word privacy, the Supreme Court judgements will act as a reference,³ where the 'Right to Privacy' was recognised as a subset of the larger part of 'right to life and personal liberty under Article 21 of the Indian Constitution. But this right can only be exercised against government actions, not for actions of non-state entities.

NATIONAL REGIMES ON PRIVACY RIGHTS OF EMPLOYEE:

The dynamic concept of privacy is interpreted differently from age to age. Art. 21 of the Constitution of India guarantees 'Right to Privacy' as a part of 'Right to Life', and this has been acknowledged by various landmark judgements. As privacy is fundamental right enjoyed by every person the employee also enjoyed certain amount of privacy at work place and right to keep personal information. But in the interest of company, companies some time may override these rights through by monitoring the activities of employees. The employer may track workers' digital footprints. They can search and have a track on employee's data, their actions and speech and know about personal lives.⁴ In the interest of protection of employee's privacy and their data, it is mandatory that the organization should have privacy policies and needs to be documented as a part of specific rules for using of personal information of employees.

At the domestic level as a part of employee rights, India is having labour codes to control the conditions of work, non-discrimination, maternity laws, payment of wages etc. The DPDP Act, is still needs to work on this subject.

In our country, the worker's privacy rights can be drawn from different legislations in the absence of specific data protection law at workplace. The following are some of the laws the address this subject.

³ Kharak Singh V/S State of U.P (AIR 1963 SC 1295) and People's Union of Civil Liberties V/S the Union of India (1997) 1 SCC 318), and the recent Puttaswami judgement (2016)

⁴ **King Stubb & Kasiva – Advocates and Attorneys, “Employee Privacy Rights in India – Understanding the Legal Framework” (May 2023). [available at <https://ksandk.com/labour/protecting-employee-privacy-rights-in-india/>]**

1. The *DPDP 2023* regulates the processing of digital personal data by safeguarding the right to privacy of individual, which includes employees on common perspective.
2. The *Information Technology Act 2000 and IT Rules 2011* regulates the personal information and sensitive personal data or information under Sec. 43 (a), (b) & (i),⁵ Sec. 43A,⁶ Sec. 66C⁷ and Sec. 72A⁸.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (IT Rules 2011) prescribes several requirements for the corporate entities for collecting, processing and storing of personal data, which includes SPDI to comply with data protection measures. These IT Rules are similar to DPDP Act 2023, but have its own deficiencies and ambiguities. Only half of these rules can be applied to very restrictive definition of ‘sensitive personal data’ which excludes other personal data; half of them do not impose obligations in relation to data subjects per se, but only to ‘the provider of the information.

➤ Employees’ Rights under IT Rules

- *Right to Correction and Access:* As per Rule 5(6), an employer [must permit employees](#), as and when requested by them, to review the information they had provided and ensure

LEGAL

⁵ **The Information Technology Act (2010), s. 43 (a),(b) and (i): any person who either, (a) accesses a computer, computer system or computer network, (b) downloads copies, or extracts any data, computer data base or information from such computer, computer system or computer network which includes information or data held or stored in any removable storage medium; (c) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource; with the intent to cause harm and without the owner’s consent (or the consent of any other person who is in charge of the computer/computer system/computer network) shall be held liable and be required under this section to pay damages of not more than Rs One Crore to the person affected.**

⁶ The Information Technology Act (2010), s. 43A: In the event that a body corporate negligently fails to implement and maintain reasonable security practises and procedures and causes wrongful loss or wrongful gain to any person while handling sensitive personal data or information in a computer resource that it owns, controls, or operates, such body corporate shall be liable to pay damages by way of compensation, which shall not exceed Rupees Five Crores.

⁷ The Information Technology Act (2010), s. 66C: Anybody who uses another person's electronic signature, password, or any other unique identification feature dishonestly or fraudulently maybe punished with imprisonment of up to three years and a fine of up to INR 1,00,000 in addition to their punishment.

⁸ The Information Technology Act (2010), s. 72A: If someone, including an intermediary, discloses information about another person without that person's consent or in violation of a legal contract while performing services under the terms of a legal contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, they may be punished with imprisonment for a term that may extend to three years or with fine extending to five lakhs or both.

that any personal information or sensitive personal data, or information found to be inaccurate or deficient, shall be corrected or amended as feasible.

- *Right to Withdraw Consent: As per Rule 5(7), an employer is required to give an option to withdraw consent at any time, in relation to the information so provided. In case of withdrawal of consent, the employer has the option not to provide the goods or services for which the concerned information was sought.*

➤ **Employer's Obligation under the IT Rules**

- a) *Lawful collection and Notice Requirements* - An employer should collect the SPDI of an employee only if required/necessary for a lawful purpose and in connection with the functioning of the employer. The information should be used only for the purpose for which it is collected and should not be retained for a period that is longer than is required.⁹

As per Rule 5(3), employer 'collecting information directly from the employee concerned' (but not otherwise), 'shall take such steps as are, in the circumstances, reasonable to ensure that the employee concerned is aware of the fact of collection, the purpose, the intended recipients, and the contact information for the collector and the party that will hold the data. Because of the broad definition of 'information in Rule 2((1)(f), this requirement should apply to all 'personal information collected from employees. Employees are not entitled to any notice when their personal data is collected from third parties.

- b) *Consent Obligations: Organizations collect, store, track and process an employee's data from the point of joining an organization to till the day that the employment contract is terminated. As per Rule 5(1), employers must obtain, before collection, written consent from the provider of the information 'regarding purpose, means and modes of use' (sensitive information only). This applies to employees as they are the provider of the information. This needs to be the case*

⁹ Sensitive Personal Data or Information (SPDI) – the organisation can collect the SPDI of workers for various reasons, which includes hiring process, record retention, employee assessments or to fulfil any other legal requirements. The confidentiality of such data should be maintained throughout the processing of data and transfer of data to third parties. The Rule 5 of IT Rules states that 'no corporate or person acting on its behalf may collect sensitive personal data or information unless the information is used for legitimate purpose to fulfil corporate activity and collected only for specific purpose and data can be collected with the written consent of the employee which is under employee surveillance.

for every step of the data lifecycle, from initial data collection to processing and even retention of data.

Without consent, the employer is not permitted to take any action on the SPDI (unless there are legal requirements or the data needs to be processed to complete the contract process). If the data is exempted from obtaining consent, the employer is still required to provide the employee a notice about this processing.

- c) Retention Requirements: As per Rule 5(4), employers may not retain information beyond when it may lawfully be used (sensitive information only). This is not the same as when the purpose of collection has expired and is a low standard of protection. An employer should retain employee personal data for at least three years, as the laws on limitation provide that civil legal proceedings may be initiated during such period. Employers are therefore required to both have and to implement such a security program and be able to demonstrate their compliance as a part of 'accountability'.*
- d) Security of Employees' Data: Rule 5(8) of the IT Rules requires employers to keep the information secure. Rule 8 of the IT Rules requires that employers shall be considered to have complied with reasonable security practices and procedures if they have implemented such security practices and standards and have a comprehensively documented information security program and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.*
- e) Data Disclosure and Cross Border Data Transfer Requirements: Employers must ensure that the country to which the data is being transferred to has the same level of data protection as is required under Rules 5(8) and 8 of the IT Rules. Furthermore, sensitive data can only be transferred with the consent of the employee, unless the transfer is necessary for performing a lawful contract between the transferor and the employee. With regards to transfers of data to third parties (outsourcing companies), the same obligations apply, which means that the organization needs to assess the third party for sufficient security controls before transfer. The same also applies to sensitive data, where employee consent must be obtained before transferring any such data unless it is required to perform a lawful contract.*
- f) Privacy Policy Requirement: Under Rule 4, an employer who collects, receives, possesses, stores, deals or handles personal information of employees shall provide a privacy policy for handling of or dealing in user information including sensitive personal information and ensure*

that the same are available for view by employees. Employees have the right to seek a privacy policy from the employer.

➤ Consequences of violation of IT Act and IT Rules

If the employer is negligent in implementing and maintaining security controls as specified under the IT Act and IT Rules, which in turn results in a wrongful loss or gain to any person, the employer has to pay compensation to the affected person. In case of violation against any other obligation under the IT Rules, employers can be required to pay compensation of up to INR 25,000 (approximately USD 350) to the persons affected by such non-compliance or to pay a penalty of up to INR 25,000 (approximately USD 350).

As a part of the duty, the employer must be mindful of the compliances and liability relating to the SPDI. If in case the employer is negligent in implementing and maintaining 'reasonable security practices and procedures' for the employee's protection, it may result in 'wrongful loss or wrongful gain' to another person.

➤ Compliances in relation to SPDI [Sensitive Personal Data and Information]

The IT Act sets out various parameters and compliances for the employer while dealing with the employee's SPDI.

- *Nexus* – SPDI will only be collected if it is needed. For eg: if the organisation involves hazardous substance related work, it will collect the detailed information about the medical records of employees to be assigned with such work. Such data can be retained until post cessation of employment. The SPDI Rules states that such data can not be retained longer than it is required.
- *Opt in and opt out* – Priorly the written consent should be taken from the employees before collecting specific data of SPDI. Along with opt in option, opt out option must be available to the employees.
- *Privacy Policy* – As per the IT Act, employers should have a well-documented privacy policy both at online and offline portal.
- *Access* – The employee must be given access to revise and correct the information.
- *Transfer* – The collected data can be transferred only with the consent of the concerned employee, provided the transferee adheres to similar data protection according to the law.
- *Reasonable security practices and procedures* – There must be Reasonable security practices and procedures which has to be maintained by the employer to protect SPDI. Such

practices may be mandated according to the law or agreed upon the parties or in such absences, it is recommended to follow Rules of International Standards such as IS/ISO/IEC 27001 [Information Technology Security Techniques, Information Security Management Systems Requirements.

In this regard, the organisation must have proper employee data protection and privacy policies (for eg., employee contracts, consent clause, company policies, audit mechanisms etc).

In case of MNCs the data will be collected and processed at single location and data is made as centralized data which can be accessed by any of the other subsidiary companies situated in different parts of the world. Hence, it is necessary for such companies to have data protection policies in coordination with relevant laws of those countries.

The employer may face certain critical issues such as data leakage, data misuse, data mining, violation of intellectual property, defamation and so on. Hence, the employee surveillance is much needed mechanism which has to be adopted by the companies. There are various techniques or ways through which the employer monitor employees (keeping in mind the legal issues associated with such ways), which includes telephone call recording, monitoring of e-mails, surveillance cameras etc.

It is challenging for companies to maintain a balance between the legitimate requirements of employers to collect & process the data and monitoring the employee activities in the interest of company as well as employee's right to privacy.

GENERAL PERSPECTIVE OF DATA SECURITY STANDARDS:

Data Security standards differs from Data protection regulations and frameworks. These standards act as a guideline which can be followed by the organisation to protect sensitive and confidential information. Adoption of such guidelines can help to prevent unauthorised access of data, its use, disclosure, modification or destruction of data.¹⁰

With the emergence of new technologies, various organisations developed different data security standards. Such as International Organisation for Standardization (ISO), National Institute of Standards and Technology (NIST) and Payment Card Industry Data Security Standard (PCI DSS). Some of these standards are mandatory, whereas some of them are voluntary, but recommended as best practices.

¹⁰ Nir Onn, "The Complete List of Data Security Standards" (February 2023). [available at <https://www.reflectiz.com/blog/data-security-standards/>]

The organisations have to come up with various data protection regulations in addition to above mentioned data security standards. The data protection regulations establish legal requirements for handling and protecting personal and sensitive information. (eg. European Union's GDPR). Apart from Data security standards and some regulations, the organisations can secure their information systems through certain set of policies, procedures and guidelines which is referred as IT security frameworks.

The Data security standards are designed to address specific risks and to protect different types of information. Here is the list of data security standards:

ISO 2700 Series – This series includes risk management, security controls and security management systems. Some of them are –

- ISO 27018 – it provides guidelines for the protection of personal data in the cloud.
- ISO 27031 – it guides on developing and implementing disaster recovery plans for information and communication technology systems.
- ISO 27037 - it provides guidelines for collecting and protecting digital evidence during a cyber incident.
- ISO 27040 – it provides guidelines for protecting stored data, including data stored in the cloud.
- ISO 27799 – it provides guidelines for protecting personal health information.

NIST SP 1800 series – The NIST is a U.S. Government agency which develops standards and guidelines for various industries. It includes different aspects of information security, risk management, incident response and supply chain security. Some of the series are –

- NIST SP 800-53 – provides guidelines for the selection and implementation of security controls for federal information systems.
- NIST SP 800-171 – provides the guidelines for protecting controlled unclassified information in non-federal systems and organisations.
- NIST Cybersecurity Framework (CSF) – it provides a common language and guidelines for managing cybersecurity risks. It is designed to be flexible and adaptable to the needs of different organisations.

COBIT – The Control Objectives for Information and Related Technology is a framework developed by the Information Systems Audit and Control Association (ISACA), which provides a set of best practices for the governance and management of IT. It covers risk

management, security and compliance.

CIS Controls – The Centre for Internet Security (CIS) is a nonprofit organisation that develops best practices for securing IT systems and networks. The CIS Controls designed to be prioritized and implemented based on an organisation’s risk profile.

HITRUST Common Security Framework (CSF) - The Health Information Trust Alliance (HITRUST) is an NGO, has developed best practices for protecting sensitive health information. It provides guidelines and requirements for securing electronically protected health information.

General Data Protection Regulation (GDPR) – the GDPR applies to organisations operating in the European Union and European Economic Area. It sets out specific requirements for collecting, using and protecting personal data and gives individuals the right to control their data.

COSO – The Committee of Sponsoring Organisations of the Trade way Commission (COSO) is a joint initiative of five private sector organisation. It provides guidance on risk management. It has developed a framework called the ‘Internal Control Integrated Framework’ that provides a set of principles and guidelines for managing risk and improving internal control in organisations.

PCI DSS (Payment Card Industry Data Security Standard) – This set of standards is not directly relevant to employee data protection standards. The PCI DSS is a security standard that applies to organisations in accepting, processing, storing or transmitting the payment card data.

SOC 1 (System and organisation Controls Report) – This standard is designed to help organisations assess the internal controls related to their financial reporting.

SOC 2 – it focuses on a business’s non-financial reporting controls related to information security, availability, processing integrity, confidentiality and privacy. It is typically used by organisations that provide cloud-based or other outsources services.

SOC 3 – it is often used as a way for organisations to demonstrate their commitments to information security.

SOC for Cybersecurity – it is designed to help organisations assess their cybersecurity risk management practices and controls.

SOC for supply Chain – designed to help organisations assess the internal controls of their supply chain partners and ensure that they are meeting the necessary controls and requirements.

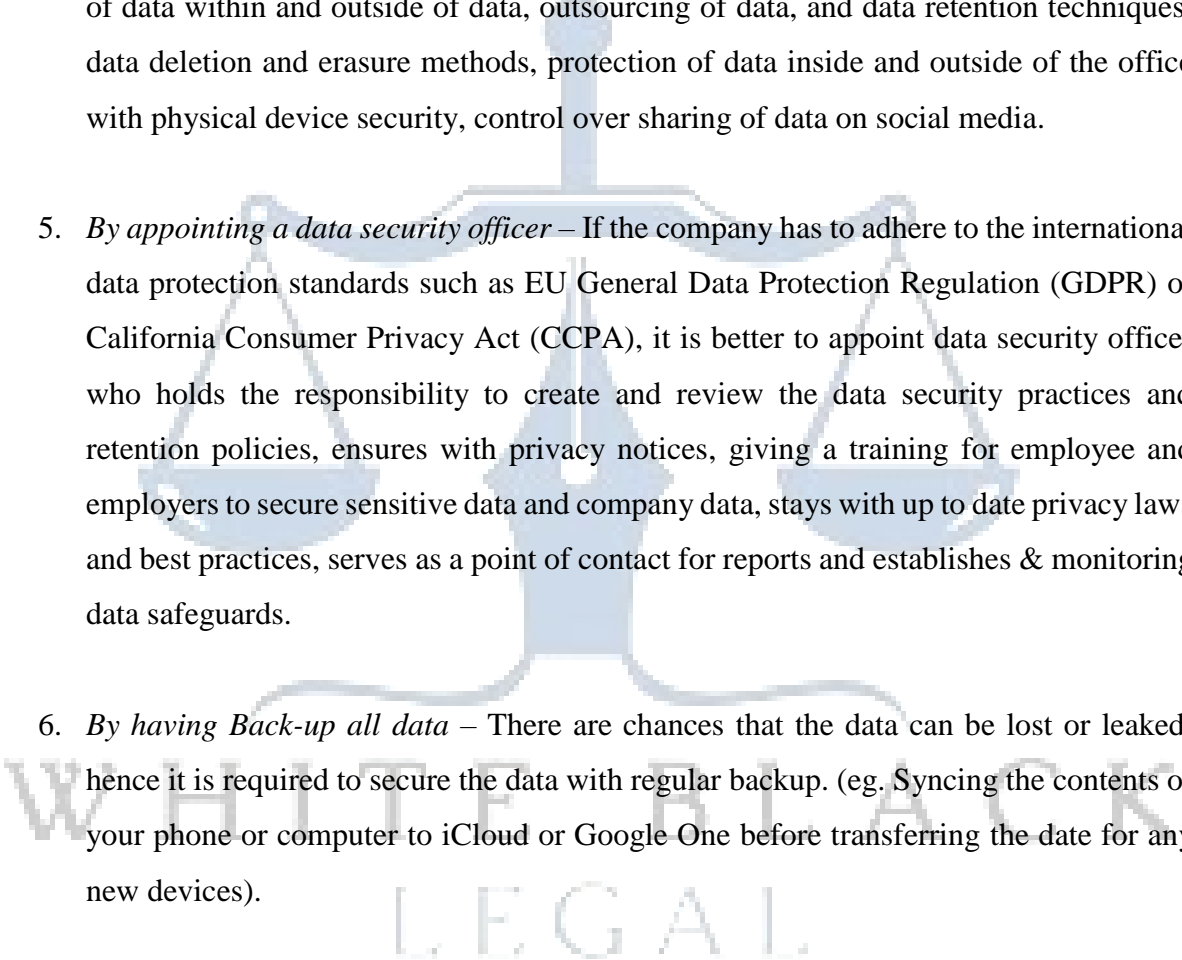
SSL/TLS (Secure Sockets Layer/Transport Layer Security) – they are cryptographic protocols that are used to secure communication over the internet.

ADOPTION OF BEST PRACTICES TO PROTECT EMPLOYEE DATA BY THE COMPANIES:

In this era of digitization, the companies need to take action to protect their employee's personal data and companies' data also. The following are some of the techniques through which the data can be protected:¹¹

1. *By establishing access controls* – the first step is to take an inventory of Personally Identifiable Information (PII) (such as social security numbers, tax payer identification number, personal contact information, bank account information, driving license and passport numbers, data of birth, race, sex, medical data, employment contracts) that the company store and process by establishing an employee data privacy program. (which includes verify employment status, issue pay-checks and system logins and so on). Secondly, establish access control mechanism, which controls the accessibility of data (who can and who cannot access the data? how much data on what purpose it can be used?). Thirdly, implement role-based permission for employee data protection. Only certain allowed users can access and process the data with specific identification login. The company can also adopt multi-factor authentication (MFA) on PII related systems, which adds an extra layer of security and makes harder for unauthorised access.
2. *By Encrypting the company data*: This is one of the methods used to protect the data. Encryption is a form of cryptography used to send secret message. It works as a protection key for your data. Such data can be accessed only with decoding or decryption method.

¹¹ Gertenbach Emily, "Protecting Employee Data: 12 Best Practices for Data Security" *Development and IT, Upwork* (August 2023). [available at <https://www.upwork.com/resources/employee-data-protection>]

- 
3. *By using antivirus and anti-malware software* – Certain viruses, malware and malicious files can hide in downloads, links and programs. Such hidden files may affect the system access code or freeze the computer or even to transfer the files to bad actors. The employees need to be trained to avoid to use invalid links, fake version programs, unauthorised e-mails, unverified free soft wares.
 4. *By implementing security policies* – Every company should have Security policies, which includes restricted access permissions, revising of new passwords, transmission of data within and outside of data, outsourcing of data, and data retention techniques, data deletion and erasure methods, protection of data inside and outside of the office with physical device security, control over sharing of data on social media.
 5. *By appointing a data security officer* – If the company has to adhere to the international data protection standards such as EU General Data Protection Regulation (GDPR) or California Consumer Privacy Act (CCPA), it is better to appoint data security officer who holds the responsibility to create and review the data security practices and retention policies, ensures with privacy notices, giving a training for employee and employers to secure sensitive data and company data, stays with up to date privacy laws and best practices, serves as a point of contact for reports and establishes & monitoring data safeguards.
 6. *By having Back-up all data* – There are chances that the data can be lost or leaked, hence it is required to secure the data with regular backup. (eg. Syncing the contents of your phone or computer to iCloud or Google One before transferring the date for any new devices).
 7. *By securing the personal devices (such as phone) connected to work devices* – The cyber security strategy can be adopted to secure the devices. There may be possibility of misuse of data or leakage of data in case if we use and connected to office devices. To avoid such threats, companies may provide the mobile, laptop or any required devices to employees to secure the data with required protection mechanism. (For eg. Cybersecurity company Cimcor recommends with usage of office devices which has remote wiping of lost devices, Role-based data access permissions, Data encryptions,

Mandatory VPN (Virtual private network) usage, Restriction on unwanted app downloads, security login apps).

8. *By outsourcing of office data securely* – While outsourcing of data relate to work for any third party (such as contractors, consultants or independent workers), it is required to include access controls such as checking the background of third parties, using contracts and non-disclosure agreements, reviewing the records of cyber security audits.
9. *By conducting security audits* – To avoid potential vulnerabilities it is essential to audit the systems and networks. The Information Systems Audit and Control Association (ISACA) recommends certain parameters that has to be included in the cyber security audits. Such as reviewing cybersecurity policies and control over data management, process of payment, GDPR compliance, having contingency plans, assessing risk levels.
10. *By monitoring network activity within and outside the company* – As attackers work very fast and their actions will be advanced. The system may be damaged before detecting the problem. So, the company should have a policy to monitor network activity in and out of the company's systems.
11. *By well preparing security incidents* – As a precautionary measure, prepare in advance to face the worst risk. Have an action plan such as personal and legal responsibilities.
12. *By working with cybersecurity pros* – The company better to have its own cybersecurity team to keep the data from hackers and other malicious actors.

CONCLUSION:

Various national laws and international standards have established the binding procedures for the processing of personal data. Priorly, ILO's Code of Practice has come up with the policies for worker's privacy rights and recently some of the countries has enacted Data Protection Laws, which includes employees' privacy rights. But, as the technology is changing every day, the new problems has also emerged, such as data anonymization, right to erase, right to consent

etc. So, there is a need to generalised principles, collection of data, processing of data, securing and storing of data and data usage. And there is a need to develop data protection provisions which specifically address the use of workers' personal data. The State need to have data protection framework for protection of employee privacy rights from threats to information privacy originating from company policies. Apart from the State laws, the companies should also lay down specific guidelines in compliance with the application of laws with reasonable expectation of privacy protection of employees.

