# Personal Data Protection in the Context of Employment: A Discussion of Law in Sri Lanka in the Light of the GDPR

RLW Rajapakse

*The Open University of Sri Lanka, Nawala, Sri Lanka*

iwrajapakse@gmail.com

**Abstract** - The right to privacy is recognized as a fundamental right in various legal instruments including international conventions. Personal data consists of a major part of privacy. Employees are a vulnerable category whose personal data may easily be misused by the employer due to the unequal power between the parties. Employee surveillances are done for many purposes such as improving employee productivity, selecting and retaining honest employees, evaluating employee performance, and maintaining workplace discipline. Under the above context, this research explored the prevailing provisions in the law on individual privacy and data protection in the employment context in Sri Lanka, in the light of the General Data Protection Regulations (GDPR) passed by the European Parliament. Special attention has been given to the public sector employment. This research study utilized the qualitative methodology where the researcher studied, analysed and synthesized a variety of materials gathered from primary and secondary sources to formulate a conclusion and to come up with the study results. Finally, the research revealed that the prevailing laws and regulations in Sri Lanka are not adequate to protect the personal data of employees; however, once the draft Personal Data Protection Bill will become an Act of Parliament, there will be an added responsibility on the part of the employer. This study fills the lacuna of having a comprehensive legal analysis pertaining to the area of employee personal data protection in Sri Lanka by suggesting how the laws should be amended to fill the gaps in the existing law.

***Keywords— personal data, data subject, data controller, employee privacy, public sector employment***

## I. INTRODUCTION

Protection of data related to individuals is felt immensely nowadays more than ever in history owing to the rapid development of electronic records of information. Personal data are gathered, stored, and processed electronically for various purposes such as banking transactions, health purposes, security purposes, statistical requirements, human resource management purposes, and many more.

Though Sri Lanka is not an exemption from this technological transformation that has embraced the whole world, still Sri Lanka is lacking in enacting separate legislation on personal data protection. A bill has been drafted with the initiation of the Information and Communication Technology Agency (ICTA) of Sri Lanka, but it has not become an Act of Parliament yet. However, as per the officials of the ICTA, the new 'Personal Data Protection Act' will be enacted very soon in Sri Lanka.

Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Convention on Civil and Political Rights (ICCPR) of the United Nations Organization recognize the right to privacy as a fundamental right. Even though Sri Lanka has ratified the ICCPR, the right to privacy has not been recognized as a fundamental right under the Constitution of Sri Lanka. However, certain legislative provisions such as Computer Crime Act (2007), Electronic Transactions Act (2006), Right to Information Act (2016), Banking Act (1988), Telecommunications Act (1991), and Intellectual Property Act (2003) may be regarded as being relevant to the right to privacy and data protection in Sri Lanka. Moreover, the right to privacy is protected in Sri Lanka as a 'delict' within the notion of *actio injuiarum* which has been developed by case law such as *Nadarajah Vs Obeysekara* (1971), *Hewamanna Vs Attorney General*(1999), and *Ratnatunga Vs. The State* (2001).

Public authorities are expected to be transparent in their exercise of power, but the same level of transparency cannot be expected from the individuals since the more transparent they are, the more they are vulnerable to unequal treatment (Right to privacy in Sri Lanka: discussion paper, 2020). Employees are

one of the most vulnerable categories of persons whose privacy rights including personal data protection rights may easily be violated in the hands of their employer owing to the huge gap of bargaining power between these two parties.

However, the right to protect personal data cannot be considered as an absolute right and it should be meaningfully enjoyed while considering other opponent rights such as the right to information, public security, public health, and employers' interests in monitoring the job tasks of their employees, etc. To strike a balance between these opponent rights, a well-defined data protection law should be there in a country. Thus, a data protection law will act as a mediator between individual interests and public interests. The General Data Protection Regulation (GDPR) passed by the European Parliament, which came into effect from 25th May 2018 in all European Union (EU) member states has become a model for non-European countries too to develop data protection laws of their own.

Under the above background, it is expected by this research to explore the prevailing provisions in the law on individual privacy and data protection in the context of employment in Sri Lanka, in the light of the GDPR. Special attention has been given to public sector employment. The assumption is that employee privacy including the personal data of them is not adequately protected under the prevailing laws of Sri Lanka. Therefore, the following research problem will be central to this study.

How does unequal bargaining power between employer and employee affect the rights of personal data protection of the employee? What have legislations done to stimulate employee privacy and personal data protection by minimizing the gap of bargaining power? Will such legislation affect the interests of the employer and how to strike a balance between employees' rights to protect their data and the employer's interests of smooth running of the business?

To unfold the above research problem, the following research questions will be examined.

What are the laws and regulatory provisions available in Sri Lanka that allow the employer to collect and process of personal data of employees?

What are the laws and regulatory provisions available in Sri Lanka on right to individual privacy and data protection?

What are the GDPR provisions on the right to protect the personal data of employees?

Is there a gap between the GDPR provisions and legislative provisions of Sri Lanka?

## II. METHODOLOGY

This is a doctrinal or non-empirical, reform-oriented research that intensively evaluates the adequacy of existing laws on data protection in Sri Lanka in the context of employment and which recommends changes to be made. The researcher reads and analyses various kinds of materials gathered through primary and secondary sources to formulate a conclusion and come up with the study results. Being primary sources, legislations of Sri Lanka including the Constitution and case law on the subject were studied and analysed to identify the gap between the law of Sri Lanka and the GDPR passed by the European Parliament. Secondary sources such as reports, journal articles, legal treaties, etc. were used to explore the importance of having enforceable laws on individual privacy and data protection.

## III. LITERATURE REVIEW

The term 'privacy' has been interpreted as a state in which one is not observed or disturbed by other people (Oxford Dictionary on Lexico.com, 2021). Privacy has been accepted as a human right under many international conventions. Article 12 of the UDHR specifically articulates that 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attack on his honour and reputation. Everyone has the right to protection of the law against such interference or attack'. International Convention on Civil and Political Rights (ICCPR- Article 17), European Convention on Human Rights (ECHR- Article 8), and Convention for Protection of Individual with Regard to Automatic Processing of Data are some other international treaties that have provisions on individual privacy and data protection.

In Sri Lanka, there is no express protection of privacy in the Constitution or other legislation, and this has been criticized as a weak point (Right to privacy in Sri Lanka: discussion paper, 2020). However, sections 53 and 54(1) of the Sri Lanka Telecommunication Act as amended by Act No. 27 of 1996 protects the privacy of people without directly mentioning it by introducing penalties including imprisonment for interception of telecommunication transmissions and the disclosure of their contents. Moreover, it is

argued that Article 14(1)(e) of the Constitution carries sufficient rationale for the Supreme Court to interpret and carve out the privacy rights (EPIC-Privacy and Human Right Report, 2006). Article 14 A (2) which has been introduced by the 19th amendment to the Constitution further clears the way of carving privacy rights since it has specifically mentioned that the right to access to information may be curtailed on the ground of privacy. Even before this amendment, in *Sinha Ratnatunga Vs. The State*, the Court of Appeal held that,

> What the press must do is to make us wiser, fuller, surer, and sweeter than we are. The press should not think they are free to invade the privacy of individuals in the exercise of the constitutional right to freedom of speech and expression merely because the right to privacy is not declared a fundamental right of the individual.
>
> The law of defamation both civil and criminal is also geared to uphold the human beings' rights to human dignity by placing controls on the freedom of speech and expression. The press should not seek under the cover of exercising its freedom of speech and expression make unwarranted incursions into the private domain of individuals and thereby destroy his right to privacy. Public figures are no exertions. Even a public figure is entitled for a reasonable measure of privacy.

This shows that the Sri Lankan courts have accepted the privacy rights of individuals though it is not specifically mentioned in any legislation.

There is a difference between the right to privacy and the right to protect someone's personal data, in the sense that, the right to privacy consists in preventing others from interfering with one's private and family life while personal data protection is the right to keep control over one's information (Lakiara, 2018). When considering this meaning, we can find no direct or indirect legislative provisions for personal data protection in Sri Lanka yet. It is expected that the draft Bill will be passed very soon since the Department of Legal Draftsman has already released the final version of the draft.

Researches done on the right to protection of personal data have suggested that employee vulnerability due to inequality of power may be misused by the employer to extract more information from an employee without his full-hearted interest or participation (Krishnan, 2006). Employee surveillances are done for many reasons such as to improve employee productivity, selecting and retaining honest employees, evaluating employee performance, etc (Krishnan, 2006). Generally, there are no contractual obligations under a letter of appointment for employers to protect the personal information of the employees, but it is the employee, who has a duty, not to disclose confidential information of the employer (Hassan, 2017). This duty on the part of the employee is evident in Sri Lanka too in the 1st schedule of Volume II of the Government's Establishments Code. It seems recent data protection laws and regulations also have not paid much attention to the rights of data protection of employees. Ogriseg (2017) argues that personal data protection is not preserved in GDPR for workers with special rules.

When searching for literature, it can be identified that there is a huge dearth of research done on employee privacy rights and employee personal data protection rights in Sri Lanka. This may be mainly due to the non-availability of a specific law on the subject. However, it is now high time to explore this area since a new Personal Data Protection Act of Sri Lanka is on its way.

## IV. DISCUSSION

According to Article 88 of the GDPR, personal data are collected and processed for many reasons in the employment context including but not limited to, recruitment, the performance of the contract of employment including discharge of obligations laid down by law or collective agreements, management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of employers' or customers' property, and exercise and enjoyment on an individual or collective basis of rights and benefits related to employment and the termination of the employment relationship.

Accordingly, it is unavoidable that data protection laws and regulations will put a huge responsibility on employers to safeguard the personal data of employees. However, Article 88 of the GDPR, which deals with the processing of personal data in the employment context, has not regulated specific rules. Instead, it requires the member states to provide for more specific rules to ensure the protection of the rights and freedom in respect of the processing of employees' personal data and such rules shall be prepared in a way that the human dignity, legitimate interests and fundamental rights of the data subjects

to be safeguarded. Though there are no specific rules in the GDPR applicable for the employment context, it can be argued that all the other basic rules in the GDPR will be applicable for this context too since the employer can be defined as 'the controller' or 'processor' within the definitions in Article 4 of the GDPR, thus the 'the employee' becoming the data subject.

Article 4(8) of the GDPR defines the term 'processor' as 'a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller'. Here, doubt arises whether a salaried employee of an organization, who has been entrusted the duty of processing of personal data of individuals, can be considered as the 'processor'. This matter will not arise in Sri Lanka in terms of the definition given for the term 'processor' under part IX of the draft Personal Data Protection Bill. The illustration given for this term in the Bill clearly shows that such an employee does not become the 'processor' and he is only an employee of the data controller. The Human Resource (HR) Department of an organization or the staff working there has been entrusted with collecting, processing, and storing of personal data of employees, but within the definition of the draft Bill, the responsibility of protection of these personal data lies on the organization, not on the HR personnel. This is the vicarious liability of the employer for the actions or omissions of its employees. However, the HR personnel may be subjected to disciplinary actions by the organization for dishonesty, breach of trust, or negligence, as appropriate, for the violation, if any, of the laws or regulations on data protection in the workplace.

As per clause (4) of the GDPR, the right to the protection of personal data is not an absolute right and it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. Accordingly, it is apparent that the employees cannot demand not to collect or process their personal data by the employer, but they can demand that the employer shall do it in a controlled manner.

There are six principles introduced by Article 5 of the GDPR for processing of personal data namely, (a) lawfulness, fairness, and transparency (b) purpose limitation (c) data minimization (d) accuracy (e) storage limitation, and (f) integrity and confidentiality. Hence, these principles will be applicable for employers too regarding the processing of the personal data of their employees. In terms of Article 6 of the GDPR, the lawful bases for data processing are consent, contract, public interest, vital interest, legitimate interest, and legal requirements. Article 13 of the GDPR requires the employer, being the data controller on one hand and the data processor on the other hand, when obtaining personal data of employees, shall provide the employees with the information such as lawful basis, the purpose of data processing, how long they are being retained if they are being shared with third parties, etc. Furthermore, only the necessary data to be obtained from the employees. On the contrary, as per chapter III of the GDPR, the employee, being the data subject, has a set of rights including the right to access and the right to have his/her data erased under certain circumstances.

These six principles as well as six lawful bases which are mentioned in the GDPR are available in the Personal Data Protection Bill in Sri Lanka too. Once the draft Bill becomes an Act of Parliament, those principles and legal bases will be applicable in the employment context in Sri Lanka too for both the public and private sectors. In terms of the principle of 'storage limitation', personal data shall not be kept for a longer period than necessary for the purpose of processing such data. The only exceptions are archiving purposes in the public interest or scientific, historical, research, or statistical purposes. This limitation is available in section 9 of the draft Bill in Sri Lanka too with the aforesaid exceptions. When considering the employment context, this limitation needs to be discussed more in the public sector sphere in Sri Lanka, since there are many rules and regulations governing the retention period of documents in government organizations such as National Archives Law (1973), Right to Information Act (2016), the Establishments Code of Sri Lanka and the Establishments Code of the University Grants Commission (UGC) and Higher Educational Institutions (HEIs).

In the public sector of Sri Lanka, almost all the personal data of employees are maintained in the personal file of the employee. According to chapter VI and clause 9 of chapter XXVIII of the Establishments Code of Sri Lanka and clauses 11 and 12 of the Establishments Code of the UGC and HEIs, there are a specific set of rules on the handling personal files and destroying them. In terms of regulations published in the Gazette No. 313 dated 31.08.1984 under the National Archives Law (1973), the personal file of a retired employee, an employee who has died, and a

casual or contract employee shall be kept for 10 years from the date of the retirement or the death as appropriate. Thereafter, those personal files can be destructed. The personal files of employees who have been dismissed from service, resigned, or sent on compulsory retirement for inefficiency shall be kept for 25 years, from the date of the termination of employment. However, the personal files of officers who had done a unique service to the organization or the country can be sent to the Department of National Archives for the purpose of archiving.

Archiving of personal data has been recognized both by the GDPR and the Personal Data Protection Bill of Sri Lanka, hence it will not be inconsistent with those regulations. However, retention of the personal data of public sector employees for 10 or 25 years after termination of their employment would be a problem with the principle of 'storage limitation'. Section 9 of the draft Personal Data Protection Bill in Sri Lanka stipulates that the period of retention of personal data shall be the period necessary for the purpose for which such personal data is processed. The only exception is the archiving purposes in the public interest or for scientific, historical research, or statistical purposes. Thus, it is in question how this responsibility put by the upcoming Personal Data Protection Act in Sri Lanka will be implemented by a public sector organization. Moreover, section 4 of the Bill stipulates that,

> It shall be lawful for a public authority to carry out the processing of personal data in accordance with its governing legal framework in so far as such framework is not inconsistent with the provisions of this Act.
>
> In the event of any inconsistency between the provisions of this Act and the provisions of any other written law, the provisions of the Act shall prevail.

When destructing any document whether containing personal data or not, the possibility of litigation shall also be considered. Accordingly, it will be lawful, for keeping the personal data of employees for a further period until the end of the term of prescription for litigation under the Prescription Ordinance, after fulfilling the purpose for which they were collected and processed. It is also argued that the prevailing rules and regulations regarding the destruction of documents of public institutes are overprotective of the interests of the employer, putting the personal data protection and privacy rights of the employee in danger.

Another area of dispute in the employment context is the right to access, right to rectification or completion, and right to the erasure of personal data by the data subject as stipulated in Article 15, 16, and 17 of the GDPR as well as in sections 14, 15, and 16 of the draft Bill in Sri Lanka. It is a question of whether these rights can be implemented in the sphere of public sector employment, as many restrictions are there in the Establishments Code and circulars in this regard. Personal files of employees are considered strictly confidential under clause 5 of chapter VI of the Establishment Code of the Government as well as under clause 30:9 of chapter III of the Establishments Code of the UGC and HEIs in Sri Lanka. Though it ensures the confidentiality of the personal data of employees, it restricted the accessibility of the employee to his own personal data maintained by the employer. As per clause 30:9 of chapter III of the Universities' Establishments Code, a university employee is entitled to access only to his history sheet maintained by the university, once in five years in the presence of an authorized officer. A similar provision was there in the clause 2:9:6 of chapter VI of the Government's Establishments Code, but after enacting the Right to Information Act in Sri Lanka in 2016, the said provision has been amended by circular No. 06/2019, issued by the Department of Public Administration. The new circular permits access to one's own history sheet without limitations as far as no inconsistency with the Right to Information Act. Since this is a requirement not only under the Right to Information Act but also under the upcoming Personal Data Protection Act, it is suggested that the relevant provision in the Universities' Establishments Code shall be amended. Similarly, clauses 7:1, 7:2, and 7:3 of chapter XX of the Universities' Establishments Code stipulate that no person employed in the UGC or a higher educational institution is entitled to obtain a copy of official correspondence or a document relating to himself or otherwise. However, in the Government's Establishments Code, the parallel provision (Clause 4 of chapter XXVIII) has been amended by the aforesaid circular No. 06/2019. Thus, this is also another place where the Universities' Establishments Code needs to be amended.

A very sensitive categories of personal data are gathered annually from the employees in the category of 'staff officer' and above, in the public sector sphere in Sri Lanka, under the Declaration of Assets and

Liabilities Law (1975). According to section 3 of the said law, the employee to whom this law is applicable shall declare the assets and liabilities of himself or herself, his or her spouse, and children who are unmarried and below 18 years old. Moreover, section 5(3) of this law permits any person to call for and refer or to obtain such declaration from the authority to which such declaration has been made, on payment of a prescribed fee. The purpose of this law must be to prevent and detect corruptions and misuses of public funds by the public officers to whom such funds have been entrusted with. Though public authorities are required to act transparently, the aforesaid provision on public employees seems unnecessary intrusion of their personal data and privacy rights. In terms of the definitions given in the draft Bill in Sri Lanka, the 'financial data' are considered as a 'special category of personal data' for which, the processing is required to be done under schedule II of the draft Bill. Accordingly, it seems section 5(3) of the Declaration of Assets and Liabilities Law is inconsistent with the requirements of the draft Bill.

However, whatever the things mentioned in Establishments Codes or domestic regulations in an organization, whether private or public, it must adhere to the rights of data subjects granted by the upcoming Personal Data Protection Act as the said Act will supersede all the other laws and regulations. Nevertheless, as mentioned somewhere else in this paper, none of these rights are absolute and need to be enjoyed proportionately considering the other opponent factors as well.

## V. CONCLUSION

Employees are a susceptible category of persons whose personal data can easily be misused by the employer. Prevailing regulatory provisions in Sri Lanka have more concern on employer privacy rather than employee privacy. The GDPR and the draft Personal Data Protection Bill in Sri Lanka also have no specific provisions regarding data protection in the employment context. However, within the interpretations given for the terms 'data controller' and 'processor', in the GDPR and the Bill in Sri Lanka, it is concluded that all the provisions in those instruments are applicable for the employment context without distinction. Since the public sector employment in Sri Lanka including the state university sector is governed by the Establishments Codes applicable to them, certain provisions of those codes will have to be amended once the Personal Data Protection Act is enacted.

It is a cardinal principle in labour law that the employer-employee relationship has built upon the trust of each other. Breaking of the said trust by the employee has always justified his termination, by the court, but less attention has been paid for the breaking of the trust by the employer. Feeling of the employee that he is untrusted by his employer will result in employee frustration with the organization. Therefore, more surveillance over the employees is done by the employer, which will lead to the ultimate poor performance of the employee. Hence, having legislative control over employee surveillance and processing of personal data by the employer will enhance the trust between two parties and thereby the employer will get ultimate benefit through increased productivity of the employees. Thus, this research supports the hypothesis to a certain extent, that employee privacy including their personal data is not adequately protected under the prevailing laws of Sri Lanka and this is more evident in the public sector sphere. It is expected that the upcoming Personal Data Protection Act will cure those issues in Sri Lanka.

## REFERENCES

*EPIC --- Privacy and Human Rights Report 2006 - Republic of Sri Lanka*. [online] Available at: <http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-28.html> [Accessed 21 April 2021].

Hassan, K., 2017. *Personal data protection in employment: New legal challenges for Malaysia*. [online] https://www.researchgate.net/profile/Kamal-Hassan-3. Available at: <http://file:///C:/Users/HP-/Downloads/PersonalDataProtectioninEmploymenFinaleditedcopy5Jan%20(1).pdf> [Accessed 23 April 2021].

Krishnan, S., 2006. *Employee Privacy at Workplace: Some Pertinent Issues*. [online] Core.ac.uk. Available at: <https://core.ac.uk/download/pdf/6443412.pdf> [Accessed 23 April 2021].

Lakiara, E., 2018. *The role of data protection rules in the relationship between HR commitment systems and employee privacy. With a special focus on Greek and Dutch corporations.*. [online] Arno.uvt.nl. Available at: <http://arno.uvt.nl/show.cgi?fid=146963> [Accessed 22 April 2021].

Ogriseg, C., 2017. *GDPR and Personal Data Protection in the Employment Context*. [online] Available at: <http://file:///C:/Users/HP-/Downloads/7573-Articolo-22859-1-10-20171214.pdf> [Accessed 23 April 2021].

*Oxford Dictionary on Lexico.com also meaning of PRIVACY*. [online] Available at: <https://www.lexico.com/definition/privacy> [Accessed 18 July 2021].

Right to privacy in Sri Lanka: discussion paper. (2020). Editorial: Colombo: Centre For Policy Alternatives.

Available at: https://www.cpalanka.org/wp-content/uploads/2020/09/Discussion-Paper-Right-to-Privacy-updated-draft-4-1.pdf> [Accessed 21 April 2021].

*Legislations & International Conventions:*

Banking Act No. 30 of 1988.

Computer Crime Act No. 21 of 2007.

Convention for Protection of Individual with regard to Automatic Processing of Data.

Declaration of Assets and Liabilities Law No. 1 of 1975 as amended.

Draft Personal Data Protection Bill of Sri Lanka

European Convention on Human Rights (ECHR)

Electronic Transactions Act No. 10 of 2006.

Establishments Code of the Democratic Socialist Republic of Sri Lanka.

Establishments Code of the University Grants Commission and Higher Educations Institutes.

General Data Protection Regulation (GDPR) of the European Parliament.

International Convention on Civil and Political Rights (ICCPR).

Intellectual Property Act No. 36 of 2003.

National Archives Law No. 48 of 1973 as amended by National Archives (Amendment) Act No. 30 of 1981.

Prescription Ordinance No. 22 of 1871 as amended.

Public Administration Circular No. 06/2019.

Regulations published in Gazette No. 313 dated 31.08.1984.

Right to Information Act No. 12 of 2016.

Sri Lanka Telecommunication Act No. 25 of 1991 as amended by Act No. 27 of 1996.

Universal Declaration of Human Rights (UDHR).

*Case Law:*

Hewamanna Vs Attorney General (1999), available at https://www.lawnet.gov.lk/wp-content/uploads/2016/11/001-SLLR-SLLR-1983-1-HEWAMANNE-v.-DE-SILVA-AND-ANOTHER.pdf (Accessed 11 May 2021).

Nadarajah Vs Obeysekara (1971) 52 NLR76, available at https://www.lawnet.gov.lk/wp-content/uploads/2016/11/052-NLR-NLR-V-76-C.-NADARAJAH-Appellant-and-H.-I.-OBEYSEKERA-Respondent.pdf (Accessed 11 May 2021).

Sinha Ratnatunga Vs. The State (2001) 2 Sri LR, available at https://www.lawnet.gov.lk/wp-content/uploads/2016/11/020-SLLR-SLLR-2001-V-2-SINHA-RANATUNGA-v.-THE-STATE.pdf (Accessed 22 April 2021).

## AUTHOR BIOGRAPHY

Rajapaksege Lalani Washintha Rajapakse is an Attorney-at-Law, Notary Public, and Commissioner for Oaths having more than 20 years of experience in the legal field. She has been graduated with an LLB Degree in 2005 from the Open University of Sri Lanka and the LLM Degree in 2012 from the University of Colombo. Presently, she is working as the Senior Assistant Registrar (Legal & Documentations) of the Open University of Sri Lanka.