Q & A

K. V. Singh
Senior Partner, Kochhar & Co.

Krishna Vijay Singh is a senior partner at Kochhar & Co., one of the leading and largest law firms in India with offices at New Delhi, Gurgaon, Bengaluru, Chennai, Hyderabad, Mumbai, Dubai, Riyadh, Jeddah, Singapore, Tokyo and Atlanta (USA). The firm represents some of the largest multinational corporations from North America, Europe, Japan and India (many of which are Fortune 500 companies) in diverse areas of corporate and commercial laws.

I run a factory in Delhi and have several apprentices working in my factory. However, some of the apprentices have been raising demand for leaves and other benefits which are being granted only to the regular workers of the factory. In view of the above, please tell us what all benefits are required to be given to apprentices under the law in force.

Please note that the employment of apprentices is governed by The Apprentices Act, 1961 ("Apprentices Act"). As per Section 18 of the Apprentices Act, apprentices are not to be considered as worker but as trainees. Please note that provisions with respect to labour laws do not apply to apprentices. Thus, apprentices are not entitled to benefits which the regular workers of your factory are entitled due to the non-applicability of labour laws on apprentices.

However, you may note that Apprentices Act has recently been amended. As per the Apprentices (Amendment) Act, 2014, an apprentice shall be entitled to such leave and holidays as are observed in the establishment. Therefore, leaves and holidays shall be the same for apprentices as well as regular workers of the factory.

We are running a factory in Gujarat. Recently we have opened a division office in Delhi as major portion of our sales are from Delhi. Our factory located in Gujarat is registered under the Employers' State Insurance Act. We want to know whether we need to obtain a new ESI code for our division located in Delhi.

Since your factory in Gujarat is already registered under the Employers' State Insurance Act, 1948 ("ESI Act") (having a 17 digit code) you need not apply for registration afresh in respect of its branch offices located in Delhi or other locations of the country. Instead, you can get a sub-code generated in respect of its branch offices which can be done online, so as to comply with the provisions of the ESI Act. Further, you may note that sub-codes need to be generated only in respect of offices located outside the jurisdiction of the Regional Office / Sub-regional office in which the main office is located.

We are dealing in Oil activity. We are having plant in Maharashtra and Rajasthan. However, we are not into oil exploring activity as ONGC or Reliance Industry is. We are just blending & filing of lubricating Oil into product such as Engine Oil, Grease & LPG. We want to apply for the Registration Certificate under Contract Labour Regulation & Abolition Act. I am visiting State Labour Commissioner Office as well as the Deputy Chief Labour Commissioner Office (Central). Nobody is answering logically on the above submission. Who is the Appropriate Government in our case? OR for that matter the Controlled Industry as specified by Central Government by way of Notification or by legislation. State Commissioner Office is saying in our case State Government is the Appropriate Government and the Central Labour Commissioner Office is saying, Central Government is the Appropriate Government, and I am running around the bush. In view of the above please reply who shall be the Appropriate Government in our case.

We understand that your industry has been notified as a controlled industry by the central government. Please note that in terms of the Section 2(a) of the Industrial Dispute Act, 1947, appropriate government for the purposes of the Contract Labour (Regulation and Abolition) Act, 1970 shall be the central government or state government depending upon who exercises the control over such industry. Since your industry is a controlled industry, central government exercises control over the same and therefore, the appropriate government in your case shall be the central government. HC

Cyber Crimes by employees

In the present era of cyber world, we have witnessed an increasing dependency on technology, which has left us open to threats of cyber crime. Recent years have seen some of the biggest cyber crimes being committed in India, including the ones where corporate houses fell prey to the illegal actions of their own trusted employees. Citibank Mphasis BPO is one of the noteworthy cases where Mphasis became victim of cyber crime which resulted in huge monetary loss caused on account of greed of its own employees. With the increase in the tendency of misusing the technology, there has arisen a need for a comprehensive data protection law to regulate the criminal activities in the cyber world. In this regard, several efforts have been made in India to enact a comprehensive data protection law. In April 2011, a set of rules known as the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("IT Rules") were framed under Section 43A of the Information Technology Act, 2000 ("IT Act") which purported to create a data privacy regime in India. However, these IT Rules have been subject to severe criticism because of the crippling deficiencies and ambiguities present in these Rules.

Business process outsourcing sector, which provides employment to a large number of educated people in India and which is also responsible for a sizable inflow of foreign exchange into the country, is at the greatest risk from cyber crimes. One of the growing concerns among these data processing companies is the vulnerability to the business from cyber threats originating from within the organization as employees misuse the sensitive personal data entrusted to them at work. Since the employees operating within the organization have a strong understanding of technology infrastructure including the safety measures put in place for prevention of cyber crimes, it becomes easier for them to hack the system as compared to external perpetrators. Perpetrators of cyber crimes may also include disgruntled ex-employees, who may misuse stolen information to cause disruption or loss to business.

One of the important reasons for the exponential rise in cyber crime is the absence of a comprehensive legislation on data protection in India. Though IT Rules have made an attempt to introduce privacy regime in India, however, these IT Rules require amendments due to several ambiguities and deficiencies surrounding them. Among the numerous controversies surrounding these IT Rules, one of the major issues which has arisen is regarding protection of personal information. The IT Rules differentiate between 'personal information' and 'sensitive personal data or information'. Personal information has been defined by the IT Rules as "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person." In this regard, it is noteworthy that the IT Rules provide ample protection for sensitive personal data or information but they do not provide sufficient protection for personal information. For instance, the consent and disclosure requirements from provider of information under Rule 5 and 6 of IT Rules apply only to sensitive

personal data or information and not personal information. In other words, personal information which can be used for identifying a person such as mobile number, name, date of birth, email-id etc. has not been given priority in the provisions of IT Rules. Therefore, the IT Rules may not act as sufficient deterrence to a company or its employees against disclosure or misuse of personal information to a third party, if such disclosure or misuse is in its interest.

Rule 3 of the IT Rules provides ample protection of sensitive personal data or information. However, the definition of sensitive personal data or information is not comprehensive and needs revision. In this regard, reference may be made to definition of sensitive personnel data given under the United Kingdom's Data Protection Act, 1988 ("Data Protection Act"). The Data Protection Act provides a wide definition of the sensitive personal data, which also includes information regarding racial and ethnic origin, political opinions, religious beliefs etc. India should also make an attempt to widen the definition by including information relating to caste, race, religion and political opinion.

The IT Rules have also been subject of criticism for making impractical provisions mandatory. For instance, Rule 5(1) of IT Rules required a body corporate or any person collecting information on its behalf to obtain consent in writing from the provider of the information regarding the purpose of usage prior to the collection of the information. It was never clear how this requirement could be made workable especially in situations which could involve obtaining consent from large numbers of people. However, this issue has been clarified by the Department of Information Technology vide a clarification issued as a press release. The clarification provides that Rules 5 and 6 do not apply to the companies "providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India." In other words, the IT Rules will not apply to the companies which have a contract with the legal entity. However, the IT Rules would apply to Indian companies that obtain sensitive personal data directly. Thus, an Indian company dealing directly with the provider of information shall have to seek written consent from the provider while collecting the information and inform the said provider about the purpose for which the information is being collected.

India's data outsourcing industry is of considerable national economic importance, but is facing legal impediments, because of the lack of comprehensive data legislation. One such legal impediment India is facing at international level is pertaining to the European Union's Data Protection Directive ("Directive"). As per the Directive, data related to European citizens can be transferred outside Europe's borders only if the legal system of the host country provides a similar degree of protection. In this regard, it is to be noted that India has not been granted "Data Secure Status" by Europe due to the lack of efficient and comprehensive data protection mechanism in the country which makes confidential information pertaining to certain sectors vulnerable to piracy and theft especially by the employees working in the companies. Considering the fact that Indian corporate houses in the data process business have access to confidential and sensitive data of individuals all over the world, which is stored by these organizations in electronic form, there is an urgent need for a comprehensive legislation that deals with data protection and privacy. Though, the IT Rules are a step in the right direction, however, these provision are not adequate, more so, as they fail to lay down the obligations upon individuals and employees who actually deal with such sensitive data or information.

In order to curb the problem of cyber crime there is a need to tackle this issue at pre and post offence level. Preventive steps to stop these crimes like setting up internal vigilance system, periodic system review by the corporate houses and educating the employees about occurrence of such crimes and legal consequences of indulging in such offences, such as under the IT Act and the Indian Penal Code, could be considered by the organizations. Additionally, organizations today also need to take steps to mitigate risks by obtaining adequate insurance cover against liability arising from cyber crime. However, nothing can substitute the need for a comprehensive legislation dealing with data protection, data theft and piracy which will also result in attaining a "Data Secure Status" for India at the international level. HC