IWIRC

connecting women worldwide

INDIA NETWORK

Quarterly E-Newsletter (January – March 2022)

MEMBER ARTICLES

Significance of Data Privacy in Evolving Insolvency Regime

Authored by Ms. Maneesha Dhir (Managing Partner) and Ms. Sneha Nanandkar (Principal Associate), Dhir & Dhir Associates

Introduction

In the present era, where our lives are controlled and regulated by technologies of all kind, user's personal and sensitive data can be misused and encashed by anyone with a single click, leaving us at the mercy of unknown third-party entities. Hence, the question arises how do we ensure protection of our personal data, especially when we are still coping with the after-effects of the post-pandemic world wherein many Industry giants are already experiencing bankruptcy?

In India, the privacy laws are sector-specific and in a fragmented form. To a certain extent, privacy laws are governed by Information Technology Act, 2000 ("IT Act") and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Data Protection Rules"). However, in absence of a specific piece of legislation, every sector specific law suffers from numerous loopholes which have, time and again, resulted in catastrophic consequences worldwide.

In the present article, we are attempting to highlight the importance of data privacy vis-a-vis the implications arising out of implementation of extant Insolvency Laws, Rules and Regulations.

What is the issue here?

When a Company goes bankrupt, the Board of Directors lose their disposition and management of the assets of the Company and a Resolution Professional (RP) under Insolvency and Bankruptcy Code, 2016 ("Code") is appointed to manage the affairs of the Company and accordingly, attempts are made to revive the Company while paying off the creditors of the Company. However, during the corporate insolvency proceedings (procedure under the Code), a RP is bound to share lot of confidential data regarding the Company, its business operations, promoters, assets etc., with multiple third parties such as Valuers, Chartered Accountants, Resolution Applicants etc. and such information may also include sensitive information pertaining to the Company, or personal data of promoters which may affect the business or value of shares / assets and the same can be misused, traded in numerous ways by such third parties. In order to prevent misuse of data, the Code coupled with its regulations prescribes certain safeguards, such as creation of data bank, timely updates, execution of undertakings with such third parties to ensure non-disclosure of confidential information etc. However, despite such precautionary measures, breach of confidential sensitive information continues to be a major concern as on date.

Recent incidents of data mismanagement

The Hon`ble Supreme Court of India has recognised the right to privacy as a fundamental right in the landmark Judgement of *Justice K.S Puttaswami & another v. Union of India*[1]. Further, Personal Data Protection Bill (PDP) has also been tabled in Parliament and is waiting its fruition and once passed, is expected to bring about a complete overhaul to India's current data protection regime.

Recently, in or around June 2021, the Insolvency and Bankruptcy Board of India (IBBI) suffered the calamitous consequences of loopholes in the Code. Owing to some internal misconfiguration of the IBBI`s new online portal, sensitive data of employees of companies undergoing corporate insolvency proceedings was leaked. This leaked

[1] Justice K.S Puttaswami & another Vs. Union of India Writ Petition (Civil) No 494 of 2012

personal sensitive information included full names, Aadhaar Card and PAN details of the employees. The IBBI later rectified the said error and had to take down some of the documents revealing sensitive information from its portal.

The National Company Law Tribunal (NCLT) had also raised its concerns regarding confidentiality of liquidation value of assets of Videocon Industries & its twelve group companies during Insolvency Process. Subsequently, NCLT asked IBBI to examine the issue in depth and ensure that the confidentiality clause was not compromised. Thus, it would suffice to state that data shared, exchanged in today's times needs to be protected at all counts and the same can be done through stringent laws & remedial measures, which is the utmost need of the hour.

Though India has adopted certain International declarations and conventions such as the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights, it has a long way to go in terms of data privacy and protection of personal sensitive information.

What are other Countries doing about it?

On the global front, the European Union, California and South Africa have enacted the GDPR Regulation (GDPR), the California Consumer Privacy Act (CCPA) and Protection of Personal Information Act (POPI Act), respectively. The GDPR recommends a new set of responsibilities for "data controllers" (entities handling personal data) and directly applies to "data processors" (entities processing personal data on behalf of the data controller). These companies are now required to have privacy policies which includes data pertaining to recipients of customers' personal data, intent to transfer such data if any, the right to withdraw consent for processing of such data etc. CCPA, requires companies to have privacy policies including information regarding customers' rights under the new privacy law and cite reasons why such data is being collected. The POPI Act is equivalent to the EU GDPR. Furthermore, the US Bankruptcy Code also prescribes preventive measures such as transfer of personally identifiable information or use, sale, lease of such information other than in the ordinary course of business is barred where a debtor has privacy notice; unless it is consistent with the terms of the privacy notice or court holds that it would not violate applicable non-bankruptcy law.

Is the Insolvency professional, a data controller?

The terms "controller" and "processor" are defined under the GDPR and in September 2020, the draft guidelines pertaining to the controller, joint controllers and processor were published by the European Data Protection Board, being the body responsible for data protection at the EU level. In a nutshell, a "controller" is someone who controls the purposes and means of the processing, i.e. the "why", "how" and the "processor" processes personal data on behalf of the controller. The terms controller and processor determine a party's legal liability in respect of personal data held or used by such person and to assess potential accountability where an individual's rights are overstepped. Thus, a RP, Liquidator, Administrator etc. fall within the concept of controller and processor, which is also dependent on the stage and activities they are involved in.

However, Indian law does not carry the concepts of controller and processor, instead the Data Protection Rules refer to the term "body corporate" and a "provider of information". A body corporate is defined as "*any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities*" wherein the 'provider of information' is a natural person providing sensitive personal information to a body corporate. The PDP bill however proposes concepts like 'data fiduciary' and a 'data processor' being equivalent to the concepts of controller and processor under the GDPR.

In the case of *Re Southern Pacific Personal Loans Limited [2013] EWHC 2485 (Ch), the* England and Wales High Court (Chancery Division) held that in creditors' voluntary liquidation, liquidators of a company were not data controllers for the purposes of the Data Protection Act 1998 which was then active. Furthermore, pursuant to GDPR being implemented in 2018, the England and Wales High Court (Chancery Division) in the case of *Green v Group Ltd & Others [2019] EWHC 954 (Ch),* once again confirmed that the administrators and liquidators are not deemed as controllers of

personal data during a corporate insolvency proceeding.

Conclusion

India needs to formulate a comprehensive piece of legislation instead of fragmented laws, rules and regulations lucid enough to ensure expeditious, hassle free and protected data transfer at the domestic as well as International level, especially since data protection transcends borders and the ever-evolving Insolvency regime necessitates the same, in order to avoid any knee-jerk reactions to unexpected infringements, breaches of personal & sensitive data content.

The Data Security Council of India (DSCI) and Department of Information Technology (DIT) must also be instrumental in establishing a Regulatory Authority ensuring timely compliances and incorporating a clear distinction of what constitutes “personal” and “sensitive data”, who can control and process the same. A fully functional redressal mechanism ought to be formed to encourage foreign as well as domestic investments to ensure smooth running of the economy.