August 2022

THE TECHNOLOGY NEWSLETTER

argus partners
SOLICITORS AND ADVOCATES

MUMBAI I DELHI I BENGALURU I KOLKATA

INTRODUCTION

The Argus Technology Newsletter discusses recent developments in technological advances or milestones or events. As lawyers, we enjoy delving into the legal nuances and implications of technological changes and analysing their impact on our clients and their activities. It is said that law always lags behind technological advances and there could be some truth behind such statement, but there is no reason for lawyers to lag behind technological advances.

The Argus Technology Newsletter is not meant to be a substitute for your regular technology periodical. Instead, we hope and promise to offer a lawyer's insights into technological change and innovation.

Argus Partners has a developed a strong and a robust technology and data privacy practice, which spans transactional advisory, corporate and regulatory advisory as well as contentious matters and disputes. Whilst physically the attorneys are based out of our Mumbai, Delhi & Bangalore offices, the team is servicing clients across the globe on Indian legal issues in technology and data privacy.

National Data Governance Framework Policy

Contributed by Vallari Dronamraju (Associate)

Introduction

In India, digitization has accelerated development, governance and led to a fast-paced digital economy. Public digital platforms are now empowering citizens, enhancing government-citizen engagement and leading to inclusive development across communities. However, it is pertinent to note that the data that is collected is inconsistently managed across different government entities and thus there is a need to implement a uniform policy that is ensuring safe distribution of data.

Aim of the Policy

The Ministry of Electronics and Information Technology published the Draft National Data Governance Framework Policy ("**this Policy**") on May 26th, 2022. This Policy aims to transform government data collection and the data management processes, with the objective of improving digital systems through a data-led governance approach. The government aims to establish guidelines, rules, and standards to build and access anonymized non-personal data to ensure the growth of Indian datasets, in order to facilitate a data led research and start-up ecosystems in India.

State governments are also encouraged to adopt the provisions of the policy and rules, standards, and protocols. The primary objective of the Policy thus includes the acceleration of digital governance, a standardized data management and security

standards system, to build a platform that will allow dataset requests to be received and processed, to set quality standards for and non-personal datasets. With the help of the India Data Management Office ("**IMDO**") that will set out a comprehensive set of standards and rules including the cloud, ministries and departments across the country can define their data storage and retention framework.

Monetary Value of Data and Data Governance

Once the monetary value of data assets is identified, it can be used as a unit of exchange in a transaction, either as sole payment or in combination with money. Therefore, the monetary value of data makes it an essential component of any business, attracting investors and valuators.

The volume and velocity of data is also improving and can be used to dictate experiences and engagement with the government. This Policy also launches non-personal data and addresses the methods and rules to ensure that non-personal data and anonymized data from both the Government and private entities, are safely accessible by research and innovation institutions. This Policy is therefore, more likely to affect researchers, start-ups and other businesses that heavily rely on non-personal datasets. This Policy will assist the Government in holding these entities accountable in the long run and enable greater transparency, accountability and ownership.

IMDO

An important component of this Policy is the IMDO which shall be set up under the Digital India Corporation ("**DIC**") under the Ministry of Electronics and Information Technology. The IMDO shall formulate all data/ datasets/ metadata rules and standards under this Policy in consultation with ministries and State Governments. It will also assist in the acceleration of inclusion of non-personal datasets housed with ministries and private companies into Indian datasets. The IMDO shall also encourage and foster data and AI-based Research, start-up eco-systems by working with the Digital India Start-up Hub. State governments are also encouraged to designate/ appoint State level officers to govern datasets according to this Policy and IMDO is to provide all assistance including training in this regard.

The IMDO will enable and build the India datasets program, which will consist of non-personal and anonymized datasets from the Government entities that have collected data from Indian citizens. Private entities are also encouraged to share such data. The IMDO must also ensure that data usage rights along with permissioned purposes will be with the data principal. The IMDO will formulate disclosure norms for data collected/ stored/ shared and accessed over a certain threshold and promote ethical and fair use of data shared beyond the government eco-system. A detailed implementation manual is also required to be published by the IMDO that includes data sharing toolkit, operational manuals, mechanisms for data anonymization and privacy.

Conclusion

This policy aims to bring in place the full potential of digital government with the aim of maximizing data-led governance that can transform the lives of the citizens in areas

that include healthcare, law and justice, education, and others. This policy will ensure data security and informational privacy, as a cornerstone for effective data-governance. On a global level, this will bring India at par with regions that already have robust data governance systems such as Europe and California and will help in the creation of an ecosystem that encourages maintaining a safe harbour for personal data used in research and development in the AI and start-up environments. Thus, the NDGFP is the first step towards building a sustainable digital government that will accelerate data-driven governance, in a data-driven economy like India.

Digital Lending Guidelines by RBI

Article Contributed by Anushkaa Shekhar (Associate)

The Reserve Bank of India (**"RBI"**) had constituted a Working Group on 'digital lending including lending through online platforms and mobile apps' (**"WGDL"**) on January 13, 2021. The report by WGDL was released by RBI on November 18, 2021, inviting comments from stakeholders.

Taking into account the inputs received, on August 10, 2022, the RBI issued a press release setting out the regulatory framework governing the digital lending in India (**"DL Guidelines"**) with a focus on RBI's regulated entities (**"RE"**), the lending service providers (**"LSP"**)[1] and their respective digital lending apps (**"DLA"**)[2].

The DL Guidelines prescribe implementation of the WGDL recommendations in a phase-wise manner with the WGDL recommendations as specified in: (a) Annex I to be implemented with immediate effect to the extent accepted by the RBI as per its regulatory stance ("**Immediately Effective Norms**"), (b) Annex II being accepted in principle but requiring further examination, and (c) Annex III requiring consideration of the Government of India and other stakeholders in view of the technical complexities, setting up of institutional mechanism and legislative interventions.

[1] An agent of a Regulated Entity who carries out for a fee from the RE, one or more of lender's functions in customer acquisition, underwriting support, pricing support, disbursement, servicing, monitoring, collection, recovery of specific loan or loan portfolio.

[2] Mobile and web-based applications with user interface that facilitate borrowing by a borrower from a digital lender. DLAs include apps of the REs as well as operated by LSPs which are engaged by REs for extension of any credit facilitation services.

Some highlights of the Immediately Effective Norms are:

1. Customer Protection and Conduct Issues

1.1 REs are required to make sure that loan servicing and repayments take place directly between the bank accounts of borrower and the RE, free from any pass-through or pool accounts from third parties. Additionally, the disbursements must go into the borrower's bank account. Exception to this being: (i) disbursals covered exclusively under statutory or regulatory mandate, (ii) flow of money between REs for co-lending transactions, and (iii) disbursals where loans are mandated for specified end-use as per regulatory guidelines of RBI or of any other regulator.

1.2 Any fees, charges, etc., payable to LSPs in the credit intermediation process shall be paid directly by RE and not by the borrower.

1.3 In an attempt to increase transparency, the DL Guidelines also mandate a standardized Key Fact Statement (**"KFS"**) to be provided to the borrower before executing the loan contract.

1.4 All-inclusive cost of digital loans in the form of Annual Percentage Rate (**"APR"**), which shall form a part of KFS, is required to be disclosed to the borrowers.

1.5 REs are required to offer a cool off period during which borrowers can exit their digital loans by paying the principal and the proportionate APR without incurring any penalties.

1.6 All LSPs engaged by REs must have a nodal grievance redressal officer to handle complaints regarding digital lending.

1.7 The DL Guidelines also provide that if a borrower's issue is not resolved by the RE within the allotted time frame of 30 days, they may file a complaint with the Reserve Bank Integrated Ombudsman Scheme (RB-IOS).

2. Technology and Data Requirements

2.1. REs have been mandated to ensure data privacy and security of the customer's personal information. Further, REs have to ensure that their LSPs do not store personal information of borrowers except for some basic minimal data (namely, name, address, contact details of the customer, etc.) that may be required to carry out their operations.

2.2. Data gathered by DLAs must be need-based, have transparent audit trails and be used exclusively with the borrower's express prior consent by disclosing the purpose thereof at each stage of interface.

2.3. Borrowers may be given the choice of accepting or declining consent for the use of certain data, as well as the ability to revoke previously granted consent, in addition to the choice of having their data deleted by the DLAs/ LSPs.

2.4. DLAs should desist from accessing mobile phone resources such as file and media, contact list, call logs, telephony functions, etc. A one-time access can be taken for camera, microphone, location or any other facility necessary for the purpose of on-boarding/ KYC requirements only with the explicit consent of the borrower.

3. Regulatory Framework

3.1. For any lending sourced through DLAs, either those of the RE or of the LSP of the RE, REs are obligated to report such lending to credit information companies (**"CIC"**).

3.2. The REs are also required to report to CICs any new digital lending products they issue to merchant platforms that involve short-term loans or deferred payments.

While the WGDL recommendations as specified in Annex II of the DL Guidelines have been *'accepted in-principle but require further examination,* the language as used in the first loss default guarantee ("**FLDG**") related paragraph suggests that this has been accepted for immediate implementation. In particular, the REs are required to ensure that pending the final determination by the RBI, the FLDGs issued to it by the LSPs adheres to the extant guidelines laid down in Master Direction – Reserve Bank of India (Securitisation of Standard Assets) Directions, 2021 dated September 24, 2021 ("**Securitisation Directions**"). While the DL Guidelines fall short of prescribing the extent of application of the Securitisation Directions on the REs and further clarity is awaited, it is expected that the Securitisation Directions will act as the baseline norms for determining which entity can provide FLDG and the extent of losses to be covered under such FLDG. This must be also looked in the context of the WGDL's recommendation to impose a complete ban on *"REs allowing their balance sheets to be used by unregulated entities in any form to assume credit risk"* without proposing any view on co-lending structures between two lender NBFCs/ banks.

With the advancement of technological innovation, the digital lending ecosystem has seen tremendous growth, resulting in various fintech organisations providing credit services. However, this expansion has resulted in exploitation of uninformed customers, unethical business practises by digital lenders, excessive participation of third parties, and concerns about the borrower's data privacy. Hence, the DL Guidelines are a welcome change in the lending market. They serve a threefold purpose:

i. They regulate the entire digital lending process while mitigating regulatory concerns.
ii. They provide transparency to the borrowers.
iii. They give importance to data privacy practices.

A quick glance at the DL Guidelines makes it evident that they are extremely borrower friendly. For example, the prohibition on (i) collection of charges which are not mentioned in the KFS and (ii) automatic increases in credit limits without the borrower's explicit approval for each such increase, ensure that the borrowers are always kept

updated regarding any decisions that could have an impact on them. Apart from this, prevention of unbridled engagement by third parties make the DL Guidelines also seem to be a step in the right direction.

The DL Guidelines also include products like 'buy now pay later' (**"BNPL"**) as a part of lending by requiring the REs to ensure that LSPs, if any, associated with such deferred payment credit products abide by the relevant RBI guidelines and by the DL Guidelines. This means that fintechs active in the microcredit category, such as ZestMoney and LazyPay, will be able to continue and expand up in the lending segment under effective regulation. On the flip side, categorizing BNPL products as loan requires the lenders to adhere to KYC compliances and mandatory bureau reporting. This has the potential to impact not only user experience because of stronger controls but may also increase costs for the lenders and restrict the flow of money. Furthermore, owing to the provision regarding direct fund flows between the RE and the borrower's bank account, third parties will now be cut off from the loan disbursal process. This will dismantle the existing business models wherein fintechs partner with banks and NBFCs in order to disburse loans, causing a significant setback to such players. However, this may also lead to the emergence of newer banking solutions.

Reserve Bank of India restricts the storage of Actual Card (Card-on-File) Data

Contributed by Arth Singhal (Associate)

As an Indian consumer, one is most likely to have come across a message on the lines of 'save card for future use' at the time of entering a payment card details on any website or app (e.g., makemytrip, swiggy etc.). In a card transaction/ payment chain, there are several participants involved who store the payment card details such as the card number, expiry date, name etc. Once these details are saved with the merchant's payment system provider/ system participant, the consumer can checkout of future transactions with ease, without having to re-enter all the card details.

At present, the payment system providers and system participants (including payment aggregators/ payment gateways) are permitted to save the payment card information, without any restrictions. However, with the increase in volume and value of transactions, the payment card information of consumers is prone to theft and fraud. There is also an additional risk of loss of privacy and theft of such data.

Restriction on storage of Card-on-File Data:

Therefore, in the interest of safety and to maintain secrecy of payment card information, the Reserve Bank of India ("**RBI**") *vide* circulars dated March 17, 2020 and March 31, 2021 on 'Guidelines on Regulation of Payment Aggregators and Payment Gateways', *vide* circular dated September 7 , 2021 on 'Tokenisation – Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services', and *vide* circulars dated December 23, 2021 and June 24, 2022 on 'Restriction on Storage of Actual Card Data (i.e. Card-on-File (CoF))', directed that no entity in the card transaction/ payment chain, other than the card issuer and/ or card networks, may

store Card-on-File ("**CoF**") data, and any such data previously stored has to be deleted with effect from October 1, 2022.

Based on discussions with stakeholders and a review of the issues involved, the RBI *vide* circular dated July 28, 2022 ("**Circular**") has directed that there shall be no change in the effective date of implementation of the aforementioned requirements and that all entities (except card issuers and card networks) shall delete the CoF data before October 1, 2022.

Interim measures:

Further, for ease of transition to an alternate system where cardholders decide to enter the card details manually at the time of undertaking the transaction, the Circular provides for the following interim measures:

a. Apart from the card issuer and the card network, the merchant or its Payment Aggregator involved in settlement of such transactions, can save the CoF data for a maximum period of T+4 days ("T" being the transaction date) or till the settlement date, whichever is earlier. This data can be used only for settlement of such transactions, and must be purged thereafter; and

b. For handling other post-transaction activities, acquiring banks can continue to store CoF data until January 31, 2023.

Tokenisation:

To further the convenience and security interests of consumers, the RBI *vide* circular dated January 8, 2019 on 'Tokenisation- Card transactions' and *vide* circular dated September 7, 2021 on 'Tokenisation – Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services', has permitted tokenisation in card transactions.

CoF tokenisation refers to replacement of actual card details with a unique alternate code called the "token", which shall be unique for a combination of card, token requestor and device. A token requestor is any entity which accepts request from the customer for tokenisation of a card and passes it on to the card network/ card issuer (i.e., the token service providers) to issue a corresponding token. This tokenisation request can be done only with explicit customer consent through Additional Factor of Authentication, and not by way of a forced/ default/ automatic selection of check box, radio button, etc.

Please find a **copy** of the Circular here.

Supreme Court orders registry to remove personal details of parties based on the 'right to be forgotten'

Contributed by Akshay Bhatia (Associate)

The Supreme Court of India ("**Supreme Court**") in an order dated July 18, 2022, has recognised the 'right to be forgotten' and 'right to erasure' as facets of the right to privacy in an application by an estranged wife ("**Petitioner**") contending that the display of her name in the public domain with respect to offences relating to sexually transmitted diseases was causing her a loss due to the social stigma associated with such diseased and thus violated her right to privacy. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 do not expressly provide for either the 'right to be forgotten' or the 'right to erasure'. Clauses 18 and 20 of the Personal Data Protection Bill, 2019 ("**DP Bill 2019**") provided for the right to erasure and the right to be forgotten respectively, but the DP Bill 2019 has now been withdrawn. In the recent past, various High Courts across the country, including the Delhi High Court, Orissa High Court, Kerala High Court and Madras High Court have been called upon to decide on issues relating to the right to be forgotten. The Supreme Court, in its landmark nine-judge decision, *Justice KS Puttaswamy (Retd.)* v. *Union of India*, had recognised the right to privacy as a fundamental right and therein mentioned the right to be forgotten.

In this case, the Supreme Court was hearing an application moved by the Petitioner in a case relating to sexual offences by the husband. The Petitioner contended that she was a victim of rape by the husband and had also charged her husband of transmitting to her an infectious disease that is dangerous to life. The Petitioner had lost before the Karnataka High Court and Supreme Court, which quashed charges against the husband on the ground that the husband enjoyed immunity under law in relation to the said offences. The two decisions of the Karnataka High Court and of the Supreme Court masked her identity, however they revealed the identify of her

husband which allowed acquaintances to link her to the case and identify her. The Petitioner also contended that the Court's judgements popped up each time someone entered key words such as 'matrimonial dispute', 'sexual offence' or any other related terms on a search engine.

The Petitioner prayed that her name be removed/ masked along with her address, identification details and case numbers so that that the same would not be available on search engines. This prayer was supported by her husband. The Supreme Court acceded to the request and subsequently directed the registry of the Supreme Court to examine the plea and work out a solution based on the 'right to be forgotten' and 'right to erasure' within 3 weeks from the date of the order.

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
argusknowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata

www.argus-p.com

Contributing Partners

Ankit Guha, Partner
ankit.guha@argus-p.com

Jitendra Soni, Partner
jitendra.soni@argus-p.com

Udit Mendiratta, Partner
udit.mendiratta@argus-p.com

Vinod Joseph, Partner
vinod.joseph@argus-p.com

MUMBAI
11, Free Press House
215, Nariman Point
Mumbai 400021
T: +91 22 6736 2222

DELHI
Express Building
9-10, Bahadurshah Zafar Marg
New Delhi 110002
T: +91 11 2370 1284/5/7

BENGALURU
68 Nandidurga Road
Jayamahal Extension
Bengaluru 560046
T: +91 80 46462300

KOLKATA
Binoy Bhavan
3rd Floor, 27B Camac Street
Kolkata 700016
T: +91 33 40650155/56

www.argus-p.com I communications@argus-p.com