PRESS RELEASE
(16.12.2021)

LOK SABHA SECRETARIAT
PARLIAMENT HOUSE
NEW DELHI

(Joint Committee on Personal Data Protection Bill, 2019)

REPORT OF 'JOINT COMMITTEE ON PERSONAL DATA PROTECTION BILL, 2019'

The Joint Committee on Personal Data Protection Bill, 2019, headed by Shri P.P. Chaudhary, MP, presented their Report today *i.e.* 16.12.2021.

The Report contains two parts. Part-I consist of General descriptions and 12 recommendations on Data Protection and Privacy in connection with provisions made in the Bill. Part-II relates to clause by clause examination of the Bill and contains 81 recommendations making modifications and more than 150 Drafting corrections and improvements in various Clauses of the Bill.

Some of the important observations/recommendations are as follows:

1. Objects and Reasons of the Bill approved

The Committee have approved the Objects and Reasons of the Bill as these are in the nature of public policy as these suitably address the concerns that emerge out of the Puttaswamy judgment on privacy as a fundamental right and the broad recommendations of Justice B.N. Srikrishna Committee.

(Recommendation No.1)

2. The new legislation will deal with personal and non-personal data both

The Committee have observed that to define and restrict the new legislation only to personal data protection or to name it as Personal Data Protection Bill is detrimental to privacy. The Bill is dealing with various kinds of data at various levels of security and it is impossible to distinguish between personal data and non-personal data, when mass data is collected or transported. So, the Committee opine that if privacy is the concern, non-personal data has also to be dealt with in the Bill. To avert contradiction, confusion and mis-management, single administration and regulatory body is necessitated. In Committee's view, all the data has to be dealt with by one Data Protection Authority (DPA). Since the Bill provides for the establishment of one Data Protection Authority, we cannot have two DPAs one dealing with privacy and personal data and the other dealing with non-personal data.

The Committee have, therefore, recommended that since the DPA will handle both personal and non-personal data, any further policy / legal framework on non-personal data may be made a part of the same enactment instead of any separate legislation. As soon as the provisions to regulate non-personal data are finalized, there may be a separate regulation on non-personal data in the Data Protection Act to be regulated by the Data Protection Authority.

(Recommendation No.2)

3. Government asked to follow a timeline for phased implementation of Data Protection Act

The Committee have noted that Clause 1(2) of the Bill does not provide for any timeline for implementation of the Act after issue of notification. The Committee have also observed

that the implementation of the Act will be in phases but feel that the period for implementation of various provisions may not be too short or too delayed. Data fiduciaries and data processors would also require sufficient time for transition. No specific provision for transitional phase necessarily creates uncertainty for the concerned stakeholders. The Committee have, therefore, recommended that an approximate period of 24 months may be provided for implementation of any and all the provisions of the Act so that the data fiduciaries and data processors have enough time to make the necessary changes to their policies, infrastructure, processes etc. The Committee have suggested that the phased implementation may be undertaken in order to ensure that within three months, Chairperson and Members of DPA are appointed, the DPA commences its activities within six months from the date of notification of the Act, the registration of data fiduciaries should start not later than 9 months and be completed within a timeline, adjudicators and appellate tribunal commence their work not later than twelve months and provisions of the Act shall be deemed to be effective not later than 24 months from the date of notification of this Act. While appointing the timelines for different phases and processes, a comprehensive analysis and consultation with stakeholders should be undertaken by the Government to discover/understand the technical/operational and managerial requirements for compliance of the provisions of the Bill. The Government should ensure that in the process of implementation of each phase, it should keep the legitimate interests of businesses in mind, so that it does not detract, too far, from the Government's stated objective of promoting ease of doing business in India.

(Recommendation No.3)

4. Committee have fixed Guiding Principles to Handle Data Breach

The Committee have expressed their concern over the forms and procedures provided for reporting of instances of data breach by the data fiduciary. The Committee have suggested some specific amendments at appropriate places in the existing Clause 25 of the Bill. Simultaneously, the Committee have also desired that there should be specific guiding

principles to be followed by DPA while framing the regulations in this regard. The Committee have desired that these guiding principles should incorporate the following points:-

(i) The Authority while posting the details of the personal data breach under Clause 25(5) should ensure that the privacy of the data principals is protected;

(ii) Where the data principal has suffered immaterial or material harm owing to the delay in reporting of the personal data breach by data fiduciary, the burden to prove that the delay was reasonable shall lie on the data fiduciary. Also, the data fiduciary shall be responsible for the harm suffered by the data principal on account of delay of reporting of personal data breach; and

(iii) The Authority should ask the data fiduciaries to maintain a log of all data breaches(both personal and non-personal data breaches), to be reviewed periodically by the Authority, irrespective of the likelihood of harm to the data principal.

(iv) Temporary reprieve to data fiduciary may also be an area of concern when data breaches occur inspite of precautions as an act of business rivalry or espionage to harm the interest of the data fiduciary.In such cases,the Data Protection Authority may use its discretion to authorize temporary order on non-disclosure of details if it doesn't compromise the interests of data principal.

(Recommendation No. 8)

5. Mechanism to be followed/decided for processing of personal data when the child attains the age of majority.

The Committee have observed that in Section 16 of the Bill, there are provisions about the processing of personal data and sensitive personal data of children, however, the Committee

have found that there is no mention of any procedure to be followed regarding delineating the options to be made available to the child at the stage when he or she attains the age of majority. The Committee have felt it necessary that there should be rules or guidelines to be followed by the data principal regarding consent when he or she attains the age of majority i.e., 18 years. Accordingly, the Committee have desired that the following provisions may be incorporated in the rules:-

(i) Data fiduciaries dealing exclusively with children's data, must register themselves, with the Data Protection Authority;
(ii) With respect to any contract that may exist between a data fiduciary or data processor and a data principal who is a child, the provisions of the Majority Act may apply when he/she attains the age of 18 years;
(iii) Three months before a child attains the age of majority, the data fiduciary should inform the child for providing consent again on the date of attaining the age of majority; and
(iv) Whatever services the person was getting will continue unless and until the person is either opting out of that or giving a fresh consent so that there is no discontinuity in the services being offered.

(Recommendation No.5)

6. Social media platforms to be treated as publishers and be regulated for the content they host

The Committee, considering the immediate need to regulate social media intermediaries have expressed a strong view that these designated intermediaries may be working as publishers of the content in many situations, owing to the fact that they have the ability to select the receiver of the content and also exercise control over the access to any such content hosted by them. Therefore, a mechanism must be devised for their regulation. The Committee have, therefore, recommended that all social media platforms, which do not act as intermediaries, should be treated as publishers and be held accountable for the content they host. A mechanism may be devised in which social media platforms, which do not act as intermediaries, will be held responsible for the content from unverified accounts on their platforms. Once application for verification is submitted with necessary documents, the social media intermediaries must mandatorily verify the account. Moreover, the Committee have also recommended that no social media platform should be allowed to operate in India unless the parent company handling the technology sets up an office in India. Further, the Committee

have recommended that a statutory media regulatory authority, on the lines of Press Council of India, may be setup for the regulation of the contents on all such media platforms irrespective of the platform where their content is published, whether online, print or otherwise.

(Recommendation No. 12)

7. Alternative Financial System to be developed in India

The Committee have observed that data protection in the financial sector is a matter of genuine concern worldwide, particularly when through the SWIFT network, privacy has been compromised widely. Indian citizens are engaged in huge cross border payments using the same network. The Committee are of the view that an alternative to SWIFT payment system may be developed in India which will not only ensure privacy, but will also give boost to the domestic economy. The Committee have, therefore strongly recommended that an alternative indigenous financial system should be developed on the lines of similar systems elsewhere such as Ripple (USA), INSTEX (EU), etc. which would not only ensure privacy but also give a boost to the digital economy.

(Recommendation No. 8)

8. Government asked to establish a mechanism for certification of all digital and IOT devices.

The Committee have noted that the current Bill has no provision to keep a check on hardware manufacturers that collect the data through digital devices. In Committee's view, with the global spread of manufacturing, it has become essential to regulate hardware manufacturers who are now collecting data alongwith the software. The Committee have, therefore, desired that a new sub-clause as 49(2)(o) may be inserted to enable DPA for framing the regulations to regulate hardware manufacturers and related entities. The Committee have strongly recommended that the Government should make efforts to establish a mechanism for the formal certification process for all digital and IoT devices that will ensure the integrity of all such devices with respect to data security. Moreover, emerging technologies, that have the potential to train AI systems through the use of personal data of

individuals, should be certified in a manner that ensures their compliance with the provisions of the Act. To achieve these objectives, the Committee have stressed upon the Government that it should set up a dedicated lab/testing facility, with branches spread throughout India, that will provide certification of integrity and security of all digital devices.

(Recommendation No. 10)

9. Government asked to bring mirror copy of the sensitive and critical data from abroad and do localization.

The Committee have observed that national security is of paramount importance and India can't compromise it on the ground of promotion of businesses. Therefore, the Committee have felt that though there are provisions under Clause 33 and 34 for cross-border transfer of data, some concrete steps must be taken by the Central Government to ensure that a mirror copy of the sensitive and critical personal data which is already in possession of the foreign entities be mandatorily brought to India in a time bound manner. Consequent upon the building up of proper infrastructure and establishment of Data Protection Authority, the Central Government must ensure that data localisation provisions under this legislation are followed in letter and spirit by all local and foreign entities and India must move towards data localisation gradually.

(Recommendation No. 11)

10. Policy to be prepared and pronounced for Gradual data localization recommended

The Committee have specifically recommended that the Central Government, in consultation with all the sectoral regulators, must prepare and pronounce an extensive policy on data localisation encompassing broadly the aspects like development of adequate infrastructure for the safe storage of data of Indians which may generate employment; introduction of alternative payment systems to cover higher operational costs, inclusion of the system that can support local business entities and start-ups to comply with the data localisation

provisions laid down under this legislation; promote investment, innovations and fair economic practices; proper taxation of data flow and creation of local Artificial Intelligence ecosystem to attract investment and to generate capital gains. The Committee have also desired that proper utilization of revenue generated out of data localisation may be used for welfare measures in the country, especially to help small businesses and start-ups to comply with data localization norms. Besides, the Committee would also like to state that the steps taken by the Central Government must guarantee ease of doing business in India and promote initiatives such as Make in India, Digital India and Start-up India. Moreover, Government's surveillance on data stored in India must be strictly based on necessity as laid down in the legislation.

(Recommendation Nos. 12)

11. Retention of data by fiduciary permitted till it satisfies the purpose

The Clause 9(1) specifically mentions that a data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of processing. Such provision is very restrictive and may be a big hurdle in functioning of the agencies which process the collected data multiple times for various welfare purposes. The Committee have, therefore, desired that in Clause 9(1) the word 'the processing' should be deleted and it should be replaced with 'such period'. Clause 9(1) may be read as under:

"9.(1) The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of (***) such period."

(Recommendation No.32)

12. Processing the data by the employer be done only if necessary or can reasonable be expected by the data principal.

The Committee have observed that the employer can't be given complete freedom to process the personal data of employee without his or her consent for the sake of employment purposes. The Committee hold the view that the relation between employee and employer is very

sensitive and should be dealt with utmost care so as no harm is caused to either of them. As employer collects all the data of its employees and there is a trust relation between them which the Committee think should be respected. Therefore, there should be equilibrium in processing of data of employee by the employer and its use/misuse of data by the employer. The employee must also be given the opportunity to ensure that his or her personal data is not being processed for unreasonable purposes. Therefore, the Committee have recommended that the processing may happen if such processing is necessary or can reasonably be expected by the data principal.

(Recommendation No. 36)

13. The creation of a separate class of guardian data fiduciary on behalf of child removed.

Besides, on the concept of "guardian data fiduciary", the Committee have observed that the difference between a child and an adult under this law is that the right to consent is exercised by the guardian on behalf of the child. So, first of all, the term 'guardian data fiduciary' needs to be defined which may be done in the form of an Explanation. Secondly, the consent from the guardian is more important and sufficient to meet the end for which personal data of children are processed by a data fiduciary. In Committee's view, the mention of guardian fiduciary will be altogether a new class of data fiduciary and there will be no advantage in creating such a separate class of data fiduciary. Moreover, the concept of guardian data fiduciary may lead to circumvention and dilution of law too.

(Recommendation No. 38)

14. Reporting of Breach of personal data within specific time directed

Clause (25)(3) is too general and does not mention any specific timeline so that the data fiduciary is obliged to report a data breach. The Committee feel that there should be a realistic and finite time frame to follow the same and to report a data breach to the Authority by the data fiduciary. The Committee, therefore, have recommended that Clause 25(3) should provide a time period of 72 hours for reporting of data breach under sub-clause (1).

"(3) The notice referred to in sub-section (1) shall be (***) **issued** by the data fiduciary **within seventy-two hours of becoming aware of such breach**.(***)"

The Committee have also noted that Clause (25)(3) in the present form doesn't put any obligation on the data fiduciary to report personal data breach to the data principal. Moreover, the Committee observe that it's not advisable to report all kinds of data breach to data principal without informing the Authority. The Committee are of the view that some data breach reports may create panic among the citizens and also affect public law and order if reported to every data principal without analyzing the exact harm to a specific data principal. Furthermore, the genuineness of trust between an individual and an entity can be questioned due to the reporting of every kind of personal data breach to data principal. Therefore, the Committee, have felt that the Authority must first of all take into account the personal data breach and the severity of harm that may be caused to such data principal and shall direct the data fiduciary to report the data principal about data breach and to take appropriate remedial measures. It is also suggested that a proviso may be added to sub-clause (5) so that the Authority can direct the data fiduciary to adopt urgent measures to mitigate any harm.

(Recommendation No. 46)

15. Qualification of Data Protection officer of International companies prescribed

The Committee have found that Clause 30 provides for conditions for appointment of Data Protection Officer. The Committee have observed that the clause simply mentions that every significant data fiduciary should appoint a Data Protection Officer who should be based in India and represent the data fiduciary in the country. The Committee have found that there is no mention of any specific qualification or position of the officer in the company. The Committee therefore, have desired that since a Data Protection Officer plays a vital role under the provisions of this Bill, he or she should be holding a key position in the management of the Company or other entities and must have adequate technical knowledge in the field.

They have also explained the expression key managerial professionals—

(i) the Chief Executive Officer or the Managing Director or the Manager;

(ii) the Company Secretary;

(iii) the whole-time Director;

(iv) the Chief Financial Officer; or

such other personnel as may be prescribed."

(Recommendation No. 50)

16. New clause introduced to devise a single window system to deal with complaints, penalties and compensation.

Keeping in view the need to devise a single window system to deal with complaints, penalties and compensation, the Committee have recommended for the insertion of a new Clause under 'Chapter X-Penalties and Compensation' to be numbered as 62. Clause 62 confers the right to the data principal to file a complaint to the Authority within such period and in such manner to be specified by regulations. It also says that the Authority shall forward the complaint or application filed by the data principal to the Adjudicating Officer for adjudging such complaint or application. Consequent upon the insertion of a new Clause 62, the Committee feel that it has to be stated under Clause 32(4) itself that the data principal, whose complaint is not resolved within the stipulated time or who is not satisfied with the manner in which the complaint is resolved or whose complaint is rejected by the data fiduciary, may file a complaint to the Authority under Clause 62. The amended Clause 32(4) may read as under:

> **"**(4)Where a complaint is not resolved within the period specified under sub-section (3), or where the data principal is not satisfied with the manner in which the complaint is resolved, or the data fiduciary has rejected the complaint, the data principal may file a complaint to the Authority **(***) under section 62."**

(Recommendation No. 51)

17. Conditions added for transfer of critical data

The Committee have noted that as per Clause 34(1)(b), the Central Government, in consultation with the Authority, has been empowered to allow transfer of sensitive personal data, for the purpose of processing and with explicit consent of the data principal, to any country with

certain safeguards such that transfer is only made to a country having adequate level of protection for the data principal. Similarly, the Authority while approving a contract or intra group scheme under Clause 34(1)(a) which allows the cross-border transfer of data, should invariably consult the Central Government. The Committee, therefore, have recommended that the word 'in consultation with the Central Government' be added at the end of Clause 34(1)(a).

The Committee are also concerned about the potential misuse of the provision of the Clause 34(1)(a) by individuals/organizations with mala-fide intentions or by foreign entities whose actions might be inimical to the interests of the State. In order to ensure a balance between the legitimate needs of businesses and the protection of the fundamental right of privacy of individuals and to protect the larger interests of the data principal vis-à-vis public policy, the Committee have suggested to insert a provision in the Clause 34(1)(a)whereby any contract or intra-group scheme allowing cross-border transfer of data, even after the consent of the data principal, may not be approved if such contract or intra-group scheme is against public policy.

(Recommendation No. 52)

18. Need of statutory body for media regulation pleaded

Clause 36(e) relates to the processing of personal data for journalistic purpose and seeks to regulate it with the code of ethics issued by the Press Council of India or by any statutory media self-regulatory organization. In this regard the Committee are of the view that freedom of expression is necessary for the functioning of the media and should not be curtailed with the coming into effect of this Bill. At the same time the privacy rights of the individual, that the Bill seeks to protect, must also be safeguarded against misuse in the name of journalism. The Committee have also felt that self-regulation by the media is insufficient and there is a need of a comprehensive code and a unified entity for the regulation of media, in all its forms and iterations in the country. The Committee have noted that at present there is no single unified agency that regulates the various forms of media, specifically news media, in the country. In the Committee's view, the existing media regulators such as the Press Council of India are not appropriately equipped to regulate journalism sector that seeks to use modern methods of communication such as social media platforms or the internet at large. In this regard, the Committee have felt that there is need for the establishment of a statutory body for media regulation in order to fulfill the above mentioned objectives. The Committee have desired that Clause 36(e) may be amended to empower any statutory media regulator that the Government may create in the future and until such time the Government may also issue rules in this regard.

(Recommendation No. 58)

19. Composition of Selection Committee for Appointment of Chairperson and Members of DPA made robust, inclusive and independent.

The Committee have desired that provision for Chairperson and Members in Clause 42(1) should be modified to make it specific and thus it may be modified stating that one Member shall be an expert in the area of law having such qualifications and experience as may be prescribed.

> **"42.**(1) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be (***) **an expert in the area of law** having **such** qualification**s** and experience (***) **as may be prescribed**."

Clause 42 (2) states that the Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a selection committee consisting of – (a) the Cabinet Secretary, who shall be Chairperson of the selection committee; (b) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; and (c) the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology.

The Committee have found that the proposed composition of Selection Committee in the Bill has only three Members and all are Secretary level bureaucrats. The Committee desire that inclusion of technical, legal and academic experts in the Selection Committee should also be made to make it more inclusive, robust and independent. Accordingly, Clause 42 (2) has been amended as under:

"42.(1) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be (***) an expert in the area of law having such qualifications and experience (***) as may be prescribed..
(2) The Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a Selection Committee consisting of—
(i) the Cabinet Secretary, who shall be Chairperson of the Selection Committee;
(ii) the Attorney General of India - Member;
(iii) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs - Member; (***)

(iv) the Secretary to the Government of India in the Ministry or Department dealing with (***) Electronics and Information Technology - Member;
(v) an independent expert to be nominated by the Central Government from the fields of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration or related subjects - Member;
(vi)a Director of any of the Indian Institutes of Technology to be nominated by the Central Government – Member; and
(vii)a Director of any of the Indian Institutes of Management to be nominated by the Central Government – Member.

(Recommendation No. 63&62)

20. Penalty provisions for data fiduciaries made flexible

The Committee have noted that flexibility in the imposition of penalty is required as digital technology is rapidly evolving and the quantum of penalty needed to be imposed would need to be decided taking into account these factors. Startups and smaller data fiduciaries engaged in innovation and research and development activities, etc. may also need to be considered separately. Hence, the quantum of penalties to be imposed may be prescribed in the rules subject to the maximum quantum as specified in this Clause. Consequently, the sub-sections (1) and (2) of this Clause may be modified accordingly. The Clause has been modified as under:

"**57.**(1)Where the data fiduciary contravenes any of the following provisions, **namely:-**
(a) obligation to take prompt and appropriate action in response to a data **(***)** breach under section 25;
(b) failure to register with the Authority under sub-section (2) of section 26;
(c)obligation to undertake a data protection impact assessment by a significant data fiduciary under section 27;
(d)obligation to conduct a data audit by a significant data fiduciary under section 29;**or**
(e)appointment of a data protection officer by a significant data fiduciary under section 30,
it shall be liable to **(***)such** penalty **(***)** **as may be prescribed, not exceeding** five crore rupees or two per cent. of its total worldwide turnover of the preceding financial year, whichever is higher.
(2) Where a data fiduciary contravenes any of the following provisions, **namely:**—
(a) processing of personal data in violation of the provisions of Chapter II or Chapter III;
(b) processing of personal data of children in violation of the provisions of Chapter IV;
(c) failure to adhere to security safeguards as per section 24;or
(d) transfer of personal data outside India in violation of the provisions of Chapter VII,
it shall be liable to (***) **such** penalty (***) **as may be prescribed, not exceeding** fifteen crore rupees or four per cent. of its total worldwide turnover of the preceding financial year, whichever is higher.

(Recommendation No. 71)

21. Single window created for deciding penalties and compensation.

The Committee have found that there is no single window system for deciding the penalties as well as compensation cases to be decided on receipt of complaint/application before the Data Protection Authority. In the view of the Committee, there must be a single methodology to decide the course of action on the filing of complaint/application. There is a provision of filing complaint to the data fiduciary by the data principal under Clause 32 and there is a provision of seeking compensation under Clause 64 by filing a complaint with the Adjudicating Officer. The Committee therefore feel that the Act should clearly lay down the procedure to be followed under both the situations. Accordingly, the Committee have desired that the DPA shall forward the complaint or application filed by the Data Principal to the Adjudicating Officer for adjudging such complaint or application. For incorporating all the provisions as suggested, the Committee desire that a separate Clause may be inserted in the Bill with a marginal heading that reads 'Right to file a complaint or application' The Committee have, therefore, recommended for insertion of a new Clause before Clause 62 of the Bill.

(Recommendation No. 73)

22. Head of the Government Departments are not made directly responsible for data breach.

The Committee have expressed their concern with respect to the capacity of Government departments to protect the large volume of data that they collect. The Committee observe that since the Government will be a significant data fiduciary, as per the provisions of the Bill, it will have to establish Standard Operating Procedures in the Ministries and Departments etc. to protect the huge amount of data that is collected. The Committee have noted that as per the provisions of Clause 85(1) and Clause 85(3) any offence, under the Act, is said to be committed by a department, authority or body of State. In the view of the Committee, actually the offence should be said to be committed by any particular government data fiduciary and not by any department, authority or body of State. Moreover, as per the provision of the Clause the responsibility of any offence under this Act is placed on the Head of the Department concerned. With respect to Clause 85(1) &(3), the Committee feel that if the responsibility for any offence with respect to the provisions of this Act, is placed on the Head of the Department, it may impede decision making process in the department. Further, this will likely create multiple hurdles in the everyday functioning of the government department. In the view of the Committee, in case of any offence under the provisions

of this Act, the Head of the Department concerned should first conduct an in-house inquiry to determine the person or officer responsible for the particular offence and subsequently the liability may be decided.

(Recommendation No. 85)