BEFORE THE HONOURABLE HIGH COURT OF KERALA AT ERNAKULAM

Writ Petition (Civil) Temporary No. 84 of 2020

Between

Balu Gopalakrishnan : Petitioner

And

State of Kerala and others : Respondents

STATEMENT FILED ON BEHALF OF THE FIRST RESPONDENT, AS DIRECTED BY THIS HONOURABLE COURT

V. MANU

SENIOR GOVERNMENT PLEADER

BEFORE THE HONOURABLE HIGH COURT OF KERALA AT ERNAKULAM

Writ Petition (Civil) Temporary No. 84 of 2020

Between

Balu Gopalakrishnan : Petitioner

And

State of Kerala and others : Respondents

INDEX

Sl No	Contents	Page No.
1.	Statement filed on behalf of the first respondent	1 to 37
2.	**Annexure – R1(a):** A true photocopy of the situation report dated 16/3/2020 of the World Health Organisation	38 to 46
3.	**Annexure – R1(b) :** A true photocopy of the study report dated 24/03/2020	47 to 79
4.	**Annexure R1(c):** A true photocopy of GO (MS) No. 79/2020/ GAD dated 20/04/2020	80 to 81
5.	Application to accept the statement	82 to 83

Dated this 22nd day of April, 2020.

V.Manu
Senior Government Pleader

BEFORE THE HONOURABLE HIGH COURT OF KERALA AT ERNAKULAM

Writ Petition (Civil) Temporary No. 84 of 2020

Between

Balu Gopalakrishnan : Petitioner

And

State of Kerala and others : Respondents

STATEMENT FILED ON BEHALF OF THE FIRST RESPONDENT

1. This statement is being filed on behalf of the first respondent, State of Kerala, as duly authorised and on the basis of the written instructions furnished. This statement is not filed in lieu of paragraph wise counter to the averments, allegations and contentions in the writ petition, but only to apprise this Honourable Court of the factual aspects of the case, for the limited purpose of admission hearing of the aforementioned writ petition. It is submitted that this statement is being filed without prejudice to the rights of the first respondent to file a detailed counter affidavit later on, if deemed necessary.

FACT SITUATION WHICH NECESSITATED THE COURSE OF ACTION NOW ADOPTED BY THE FIRST RESPONDENT

2. The entire world is facing an unprecedented crisis because of the COVID – 19 pandemic. The medical fraternity and the scientific community have not so far been able to find out any medicine or vaccine for the same. There is also no human anti body identified so far. Even the most advanced countries of the world in Northern America and Europe are finding it difficult to contain the spread of virus. COVID -19 is of highly contagious nature. It is estimated that each affected person transmits the virus to 2 to 3 people with whom

he comes into contact with. Though the mortality among young patients is low, the mortality is as high as 2 to 3 % in the case of old people above 70, if the patient has other co –morbidity conditions like Blood Pressure, Diabetes etc. The only method to contain the disease is to keep away from one another.

3. Ever since the first COVID – 19 case was reported, the first respondent, State of Kerala, took all steps to ensure proper identification of persons affected, their primary and secondary contacts and those who are likely to be affected and ensured their continuous and rigorous observation. Any person identified with COVID symptoms, while in isolation, will be hospitalised. The Government of Kerala (hereinafter referred to in this statement as "the Government" for short) also used the advents in information technology for the same. The Government quickly initiated measures like the GoK direct App, which became the single source of information dissemination. The Government also interacted with the Telecom Service Providers in the State and requested them to ensure sufficient bandwidth as the internet usage was bound to increase due to the increased online activities and Work from Home measures.

4. The key measures adopted in the first phase included the tracking and tracing of the persons who visited /arrived from COVID affected countries/regions. The initial thrust was on identifying and quarantining the Air travellers from the regions like China and East Asian countries like Singapore, Thailand, Malaysia and Japan. Subsequently, Italy was also included in the list. But, later, all persons travelling from or having a recent travel history from the affected regions were identified. The strategy was to ring fence these persons until it was sure that they were not affected by COVID 19, by around 14 days of self quarantine and hospitalisation of persons who showed any symptoms.

5. The Government formulated a two pronged strategy of isolating the primary and secondary contacts, keeping the identified patients in home isolation/ hospitals and putting the vulnerable under reverse

quarantine. There were clearly 2 sets of persons who needed to be addressed, those were,

1. persons under isolation /Quarantine /treatment.
2. persons who were Vulnerable (Aged above 60, those who were taking treatment for non communicable diseases, under immune suppressant drugs)

6. The Kerala Spatial Data Infrastructure, under the aegis of Kerala State Information Technology Mission, mapped the entire aged population of Kerala panchayatwise, so that geospatial data was made available for the District Collectors, Panchayats and at the State level to view the concentration of aged population, through a colour coded GIS map. The manual registers kept at each Public Health Centres, containing the details of the senior citizens under medication for lifestyle diseases or under palliative care, were digitised voluntarily by the Akshaya entrepreneurs all over Kerala in a matter of 2 days. This data was also made available to the District authorities so that they could be isolated before hand as they constitute the more vulnerable population.

7. With the primary contact list increasing and a larger number of people reporting as under risk, the Government aggressively focused on the strategy of reverse quarantining, where the most susceptible groups in the society were directed to impose a self quarantine. This included the persons above the age of 60, persons with existing life style ailments like hypertension, Diabetes etc and persons who were on critical care or under treatment with immunosuppressant drugs. It was in the context of increasing cases and more number of contacts under quarantine that the Local Self Government machinery identified ward level voluntary teams to reach out to the persons in quarantine and isolation and check their well being and ensure that they were properly taken care of and their symptoms were regularly monitored and that all directions from health authorities were complied with.

8. Currently, the Government has developed an Information Technology system, named "Corona Tracker", to collect the data of persons under isolation through the Health Centres under the Department of Health.

The list of patients is being consolidated and entered at District level through Integrated Disease Surveillance Project cell with the help of Staff from Kerala State Information Technology Mission. This helps in getting consolidated data Panchayat/District wise. Dash boards are available at every level so as to make decision making easier. The Technical Assistants from Panchayats help in data entry reducing the burden on the health personnel. The coordination is done by the District Technical Officers of Information Kerala Mission.

9. The first case of COVID19 in India was reported on 30th January, 2020, originating from China. As of 26th March, 2020, the Indian Council of Medical Research and Ministry of Family Welfare confirmed a total of 649 cases in the country. As per the Situation Report dated 16/3/2020 of the World Health Organisation, there were 1,67,515 confirmed cases of COVID -19 affected persons all over the world, with 6606 deaths. The disease was spreading at a fast pace all along the world. A true photocopy of the situation report dated 16/3/2020 of the World Health Organisation is produced herewith as **Annexure – R1(a)** .

10. It was assessed by the Crisis Management Group of the Government that there was a possibility of a sudden spike in the numbers in the first respondent State. The risk of spread was very high in the State, with a high density of population and exposed to the whole World on account of the presence of expatriate Keralites all over and also on account of being a tourist destination. Various study reports indicated the progression of COVID, once it starts affecting a State or a Country. The graphical representation very clearly indicates the sharp spurt, exponential growth and rising curve of the disease. The first Kerala specific study was the study report dated 24/03/2020 of a group of experts associated with the Centre for Disease Dynamics, Economics and Policy, John Hopkins University and Princeton University. As per the said study report, about 80 lakh people in Kerala would be affected with COVID between 28.03.2020 and 25.04.2020. A true photocopy of the study report dated 24/03/2020 is produced herewith as **Annexure – R1(b)** .

11. It was assessed by the Government that if 80 lakh people in Kerala would have been affected, about 10 % of them (8 lakhs) would have to be hospitalised and a 10 % of the hospitalised persons (80,000) would require ventilators. Going by the then available statistics, the State Disaster Management Authority (SDMA) assessed that there would be 48 lakh Peak Symptomatic Cases in the State by July end with 4.8 lakh Peak Hospitalization Cases and 36000 Peak ICU Cases, if it was low spread of the disease in the State. If it was medium spread, the figures assessed by the SDMA were 65 lakh, 6.5 lakh and 49000. If it was severe spread, the figures assessed were 82 lakh, 8.2 lakh and 62000. The SDMA had also assessed the situation, based on the pattern of the spread of the virus in Italy and Spain, and predicted that 1.25 crores virus infections could take place in the State in three weeks; that two –third of the virus affected people (90 lakhs) would exhibits symptoms; that nearly 9 lakhs would have to be hospitalised; and that about 2 lakhs would have to put to intensive care. It was also predicted, based on the pattern in Italy and Spain, that out of the 28 lakhs aged people in the State, 21 lakhs people would be affected; that 4 lakhs aged people would have to be hospitalised with atleast 2 lakhs in intensive care. The Crisis Management Group of the Government was faced with a dangerous situation like never before, unique by the sheer volume of threat.

12. Even during the early days, when there was no panic situation with the pandemic still to affect the State, the Government felt it necessary to compile the list of travelers coming to Kerala from outside the country, through Air, identify people who are coming from countries which subsequently became COVID hot spots, locate them in Kerala at their residential addresses and continuously monitor them. The physical handwritten forms collected from passengers were one source of data. This was found insufficient as there were data gaps with respect to port of origin and residential address. As such, passenger manifest from Airline companies were requested. But, each airline had a different format and data aggregation was difficult. Though, finally, information was obtained from Bureau of

Immigration, cross checking the same with passenger manifest or the arrival forms was virtually impossible with around 150000 records to be verified. Deduplication of names or actually locating a person on the ground was also a big challenge. This was a clear instance where it was felt that the situation could be handled efficiently and speedily by a big data handling framework which can be quickly customized.

13. When there is a sudden panic situation, people resort to all channels of communication to reach out to the authorities for support and help. This meant multiple numbers of chats, sms, email etc and increased usage of social media platforms for the same. Such duplication of communications creates confusion and makes tracking the needy difficult. This, in turn, delays the relief process and is an impediment to assuring that the resources are sent to the right place. It is submitted that smart phone penetration in Kerala is approximately only 70 % of the mobile users and 30 % still rely on ordinary mobile phone. This meant that 30 % of SOS messages would be by way of conventional phone calls or sms. The unstructured data thus received had to be converted to a structured format available in real time. In these circumstances, a multichannel communication network, which could handle volumes of structured and unstructured data and pass on to supporting Information Technology systems, was necessitated. Further, the fast spreading nature of COVID 19 demands a swift data collection platform at every place, which will be easy and safe for data collection personnel as well as every person under quarantine and treatment

14. To assist such processes where large volume of data would be required to be analysed and to establish a constant channel of communication with these persons, it was decided to use the support of a scalable Information Technology system. The Government owned/ controlled entities like the C-DIT and Information Kerala Mission are not technically equipped to manage such large volume of data and hence there were no viable alternatives within the Government framework. The issue had to be resolved in the shortest possible time and the circumstances necessitated extraordinary steps

on behalf of the Government. Any invitation for tender would have been time consuming in so far a technical committee ought to have ascertained the pre qualification criteria, for which atleast two weeks would have been necessary; then a pre qualification bid had to be called for, then technical bidding process would have to be undertaken; then a pre-bid meeting would have to be held, and then selection would have to be made, all these processes consuming another month. Time would have taken for grant of administrative sanction and technical sanction. The Government, on account of the alarming situation, had not time to spare. Even a day's delay would have been fatal. The third respondent showed interest in working with Government to tackle the issue. They had the experience of creating user experiences for corporates and had the technology capabilities to pull this out fast. It is a data analytics company with capability of processing large volumes of data. It's product capabilities will help the State of Kerala in:

- Enriching the identified vulnerable population (to be reverse quarantined) data
- Establishing effective communication channel with reverse quarantined people
- Engaging with the reverse quarantined (suggesting precautions, answering questions, etc.) and monitoring their health
- Reporting geospatially on the health of reverse quarantined in the State
- Identifying vulnerable, requiring focussed attention based on insights and engaging with them

15. It is submitted that the Government had earlier reached out to Global Malayalee Diaspora, particularly those who were holding key positions in various Corporates, to attract investments to the State. As per the advice of the High Powered Digital Advisory Committee of the State, made up of technocrat businessmen who could find success

by operating their businesses in the State, the Government held "#Future", a conclave for developments in the area of technology. The said Flagship Event of the Government, held in 2018, was a great success and it saw participation from expatriate Keralites across the world. In furtherance of the said event, follow-up meetings were being held in smaller clusters across the globe. The Government intended to show case the business avenues in the State through such meetings. It was through such meetings that the Government came into contact with the third respondent, as in the case of other Corporates wherein Keralites were occupying key positions. During the early days of COVID 19 itself, the third respondent had offered to work along with the State to support its cause. The offer by the third respondent was looked into and found reasonable (zero cost during COVID 19). It is submitted that that the third respondent is also a pro bono partner of the World Health Organisation in developing its COVID -19 Update dash board.

DETAILS OF DATA COLLECTED AND THE NECESSITY FOR COLLECTION OF SUCH DATA

16. There are five types of data collected, for which there are five separate forms

a) Data related to international travelers

b) Data related to domestic travelers

c) Data related to health workers or people who have contact with patients

d) Vulnerable people data –either self reported or reported by relatives

e) Data collected by field worker

17. The first 4 forms (*in relation to data (a) to (d) stated above*) pertain to voluntary self reporting by individuals. The user is properly informed in the terms and conditions that the data will be used for the COVID purpose only. The contention of the Petitioner therefore that persons submitting data online, do not have a choice is patently

incorrect and misleading. As set out above, the online submissions are through a voluntary self - reporting process.

18. The data, numbered as the fifth, is being collected by health workers when they visit homes to observe people in quarantine. The data collected through Form 5 (house visit form) is intended to identify any COVID related symptoms from among those under surveillance, so that the local self government can take note of that and can act immediately through the Public Health Centres; and to identify if any vulnerable citizens are there at the houses where citizens undergoing surveillance are there, as they can be instructed to be under strict reverse quarantine measures. Information regarding medication being taken for other illnesses such as blood pressure, diabetes etc is taken because it has been empirically established that the virus has a high mortality rate amongst persons with such pre-existing diseases. The information is therefore relevant to curbing spread of the disease and also for ensuring that medical care reaches the persons who are most susceptible to the disease. The information is being used only for the limited purpose of preventing disease and promoting public health and there is no misuse of the same. The said form is used to collect data only from people in isolation who have high vulnerability for COVID19, so that the collection of this data is extremely essential for preventing the spread of the epidemic as well as to support the Government's effort to control the epidemic. This form being collected physically is not within the purview of the Information Technology Act, 2000 (as amended) (hereinafter referred to as the "IT Act" for short), at the stage of collection. The said process is also being undertaken as a process of governance by the State.

19. With respect to the first four forms for voluntary disclosures online, the above said web forms were designed basically to ensure the essential service delivery and identify any early evidence of community transmission, which is an essential step the Government is required to take in public interest. The data fields, interalia, include the following:

1. Name, age , District, Panchayath, Ward and details of persons who were isolated (not COVID patients)
2. Details of travel to other countries
3. Any symptoms in the isolated persons (critical for ensuring testing)
4. Presence of old age persons in the house to ensure medicines.
5. Any patient who is not getting medicines. (yes/No)
6. Details of any flu like illness in the house or surrounding (As a surrogate marker of community transmission since rapid test is not in place)
7. Details of any quarantine breach and travel. (ensure quarantine for containment)
8. Any unusual occurrences in the community (surrogate evidence of community transmission)
9. Details regarding the co morbidity and NCS like Blood Pressure, Heart diseases, other diseases etc.

20. It is most humbly submitted that the questions regarding diseases is intended to gather only generic names of the diseases and not the degree of severity. It is also submitted that this information has a direct correlation to possible sources of infection and spread of the virus, as well as vulnerability to the infection. The contention in the writ petition that the details regarding the beneficiaries of the public distribution system is allegedly stored with the third respondent, is wrong.

21. During the last floods also, the local governments were the key players who were the game changers by ensuring services, medical help and necessary interventions at the right time. It is important that the local governments are equipped with data at their fingertips for taking action. Collating this data collected and comparing it with other available data and giving necessary pointers to the local government requires a competent software tool. Apart from the local body level interventions facilitated through such data aggregation, the District and State level administrations also would need reliable

and timely aggregated information to plan and implement effective strategies.

22. Of the 14 districts and around 1100 local bodies, only less than 100 Panchayats reported either COVID positive or home isolation, i.e. 10 percent of the total local bodies. If the epidemic is confined to a few geographical areas only, then the entire process of close monitoring of people in home isolation and tracking, when they become symptomatic, can be effectively carried out as being done now. During March – April period, only 2,00,000 people were under home isolation and surveillance. However, if the numbers raise to more than 20 or 30 lakhs (which actually is the number likely to be kept under reverse quarantine, being the number of elderly people and people who are immuno compromised), then the present manual system of home visit and surveillance will not be sufficient. Ideally, the individual under self isolation must be able to self report. Such self reports have to be aggregated Panchayatwise, District wise and State wise and the areas, where more focus is required, have to be identified. Such information can be effectively compiled, collected, analysed and strategized only on the basis of a strong big data Information Technology Platform, which can process and analyse such data. Then only, the resource deployment can be planned in each Panchayat. At the district level, the district administration would need to allocate resources, volunteers, treatment teams, medical resources to these vulnerable local bodies based on the pattern of spread.

23. The data collected was essential for giving the following inputs to State Executive Committee of the Kerala Disaster Management Authority, which are essentially required as per the provisions of Sections 22, 23 and 24 of the Disaster Management Act, 2005 (hereinafter referred to in this Statement as "the DM Act" for short) and the Kerala Epidemic Disease Ordinance 2020(hereinafter referred to in this Statement as "the 2020 Ordinance" for short).

1. To examine the vulnerability of different parts of the State to different forms of disasters and specify measures to be taken for their prevention or mitigation.

2. To lay down guidelines for preparation of disaster management plans by the departments of the Government of the State and the District Authorities.

3. To provide shelter, food, drinking water, essential provisions, healthcare and services in accordance with the standards laid down by the National Disaster Management Authority and State Disaster Management Authority

4. To inspect the persons arriving in the State by air, rail, road, sea or any other means or in quarantine or in isolation, as the case may be, in hospital, temporary accommodation, home or otherwise of persons suspected of being infected with any such disease by the officers authorized in the regulation or orders

5. To coordinate and monitor the implementation of the National Policy, the National Plan and the State Plan.

24. The Petitioner does not take issue with the collection of data by the Government per se. However, he has raised concerns about sharing of this data, which allegedly contains sensitive information about citizens, with the third respondent and the possibility of misuse of such data. Neither of these concerns are justified, as elaborated herein below.

HOSTING OF DATA

25. As regards hosting the data being collected through the platform/ software to the citizencentre.sprinklr. com, it is submitted that after initial testing, this was changed to citizencentre.Kerala.gov.in subdomain. As far as fifth form is concerned, the data is collected by health worker when she visits the people and it was also initially uploaded to citizencentre.sprinklr.com. This has now been migrated to citizencentre.kerala.gov.in It is important to note that in all these cases, data is stored in cloud, which is Amazon cloud in Mumbai, India and not

abroad. It is also pertinent to note that data was being stored in encrypted form.

26. The data collected through the 5 forms, as mentioned above, needs to be housed in a cloud for better configurability and scalability. A SAAS (Software as a Service) Platform, which the third respondent has offered, also needs to be deployed in the Cloud.

27. The Government had examined feasibility of using the State Data Centre (SDC) for the above. The third respondent's software require amazon tools for its processing and since SDC uses VM ware web services, this was not possible. CDIT has an Amazon cloud services account but the capacity was not enough for hosting the large volume of data expected to be collected. Hence, the Amazon cloud services account of CDIT was upgraded and the data along with application is migrated to this space subsequently. Even though the proposal of the third respondent included free hosting services, Government has planned to keep the data in its own account in-spite of the additional cost involved. Moreover, the third respondent has created a separate instance of their application in the CDIT account of AWS (Amazon Web Services), which means the said instance of the platform of the third respondent used for processing the data collected above is also in the CDIT account. It is submitted that the Government has now full and exclusive ownership of the data and for analysis of data, dedicated instance of the software of the third respondent which is now available within the CDIT will be used.

28. A large data analytic company like the third respondent was selected primarily to ensure support under two scenarios a) a large inflow of people from other parts of India and abroad once lockdown is relaxed; b) in case of a sudden spurt in disease incidence which needs to be carefully managed. In both these cases, large quantity of data in multiple formats will be reaching Government and there is a requirement for a company with Big data management and analytics capability to process the same. In these emergent circumstances, where time was of the essence, the third respondent was chosen. The work so far has been done

on an experimental manner to ensure the readiness of the platform for such eventuality. It will not be feasible for a Government agency to develop such scalable platforms and solutions in a very short period of time, as they are not specialists in this field. Further, the Government is not in a position to carry out any experiments or take any risks on account of the extra ordinary situation prevailing due to the pandemic. The need of the hour has necessitated the steps now taken by the Government. The same are also necessary to tide over the crisis which may loom large over the State on account of the return of our people from COVID hot spots all over the world, once the lock down is over. Any failure in this regard may have a telling effect on the State, especially taking note of the fact that there are two million Non Residents Keralites in Gulf alone, a quarter of which is expected to return to the State.

29. The State is gearing up all its facilities to receive our brethren from abroad and, in these circumstances, the system now developed with the third respondent, is absolutely essential and necessary. When the large inflow of people happens to the State, there is a need for properly isolating the people and managing surveillance of such people. There is a need to assess the health status of such people and control and track their movement. Moreover, in the eventuality of the spread of the disease, the most important people we need to protect are the old and vulnerable people. All this requires a strong platform for processing and analysing large volumes of data in multiple formats. The work so far done was to understand the pitfalls, challenges and areas of improvement etc, to ensure that the system is ready in all aspects once the eventuality (either mass inflow or disease incidence or both) occur. The Government has used only a very small sample set of data so far using the software and before the system goes in full form, additional procedural modifications will be implemented.

DATA SECURITY

30. As per the Order Form placed by the first respondent with the third respondent for the product Citizen Experience Management, the first

respondent is under no obligation to pay for the services rendered by the third respondent during the COVID -19 Pandemic. Upon the conclusion of the scoping and implementation, the third respondent is to provide the first respondent with pricing and at that time, the first respondent, in its sole discretion, determine what amount, if any, shall be paid. It therefore cannot be said that there is any undue drain from the Government exchequer which is contrary to public interest.

31. The terms and conditions of the Purchase Order Form and the agreements referred to therein as well as the Non Disclosure Agreement ensure that the data is secure and the right to privacy of the citizens is protected.

32. The Additional platform Terms in the Order Form specifies at paragraph 3: "*Customer shall at all times retain all rights to and responsibility for Customer Data uploaded to or accessed by the Platform. "Customer Data" is defined as any and all data used for provision of the Sprinklr Services that is obtained by Sprinklr directly from Customer, including, without limitation, the Content and all citizen data accessed or obtained by Sprinklr from Customer. Customer expressly represents that it has the legal right to make such data available to Sprinklr for the purpose of providing the Services, and agrees to indemnify and hold harmless Sprinklr and its officers, directors, and affiliates from any associated with Sprinklr's access to and use of such Customer Data. Upon termination of the services, or at any time upon Customer's written request, all Customer Data will be removed from the Platform and returned to the Customer, pursuant to Section 3.4 of the agreement.*"

33. The Master Services Agreement ("MSA") in the Order Form contains mutual confidentiality obligations. This document is incorporated by reference to the aforementioned Order Form that was executed on 2 April, and controls the data confidentialities and protection issues

MSA Confidentiality Provisions

8.1 "Confidential Information" means: (i) business or technical information, including product plans, designs, source code, marketing plans, business opportunities, personnel, research, development or know-how (all of the foregoing as they relate to the Sprinklr Services, including the Platform (current or planned), are Sprinklr's Confidential Information, and all of the foregoing as they relate to Customer's business, are Customer's Confidential Information); and (ii) information designated by the disclosing party as "confidential" or "proprietary" or which, under the circumstances taken as a whole, would reasonably be deemed to be confidential. Confidential Information includes information disclosed prior to or during the Term of this Agreement. Confidential Information shall not include information which: (i) is or becomes generally available to the public other than as a result of wrongful disclosure by the receiving party; (ii) is or becomes available to the receiving party on a non-confidential basis from a third party that rightfully possesses the Confidential Information and has the legal right to make such disclosure; or (iii) is developed independently by the receiving party without use of any of disclosing party's Confidential Information and by persons without access to such Confidential Information.

8.2 Customer and Sprinklr each agree not to use any Confidential Information of the other party for any purpose other than as necessary to perform its obligations under this Agreement. During and after the Term, neither receiving party will disclose any Confidential Information of the disclosing party to any third party without the prior written consent of the disclosing party, except (i) where such disclosure is necessary for the performance of the receiving party's obligations under this Agreement; or (ii) as may be required by Laws (provided that the party obligated to make the disclosure shall give the other party advance notice of such requirement to the extent legally permitted). Each receiving party shall be responsible for compliance with this Section and applicable provisions of this Agreement by its employees and

> Contractors, and shall obtain the agreement by each employee and Contractor to keep the Confidential Information of the disclosing party confidential and to use it solely as required for the performance of the receiving party's obligations hereunder. For purposes of clarity, Customer may publicly disclose the fact that it is using the Sprinklr Services, but all details about the uses, functionalities or other aspects of the Sprinklr Services (including screenshots and specific features of the Platform) are Confidential Information of Sprinklr and may not be disclosed.

34. The said Master Services Agreement, forming part of the said Order Form, also provides as follows:

> 2.1 Customer owns all right, title and interest in and to all Customer Content uploaded, stored, processed or transmitted through the Platform under the Sprinklr Account.
>
> 3.4 Within thirty (30) days after the effective date of termination Sprinklr will, upon Customer's request, extract all available Customer Content from the Platform. Both parties will agree to an acceptable transfer methodology, (typically Sprinklr provides an SFTP for the transfer). If Customer accounts are deactivated prior to the termination date, data contained within those accounts is not available anymore, therefore Customer must extract the data prior to deactivating accounts. After such thirty (30) day period, Sprinklr shall have no obligation to maintain or return any Customer Content. Any reasonable expenses incurred by Sprinklr as a result of this extraction shall be the responsibility of Customer

35. Clause 5 of the Mutual Non Disclosure Agreement states as follows:

> 5. MAINTENANCE OF CONFIDENTIALITY
>
> The receiving party will maintain the confidentiality of the disclosing party's Confidential Information with at least the same degree of care that it uses to protect its own confidential and proprietary information, but in no event less than a reasonable degree of care under the circumstances. The receiving party will not disclose any of the disclosing party's Confidential Information to employees or to any third parties except to the receiving party's employees and subcontractors who have a need to know such information in connection with the Purpose and have agreed to abide by non-disclosure terms at least as protective of the disclosing party's Confidential Information as those set forth herein.

36. The relevant Clauses of the Privacy Policy of the third respondent read thus:

> (3) Relevance
>
> Sprinklr will collect only as much personal information as is required to
>
> meet the specific, identified purposes of Customer contracts, and we will
>
> not use it for other purpose without obtaining your consent.
>
> (4) Retention
>
> Sprinklr will keep your personal information only as long as we need it for the purposes for which we collect it, or as permitted by law.
>
> (7) Security
>
> Sprinklr will take appropriate physical, technical and organizational measures to protect your personal information from loss, misuse, unauthorized access or disclosure, alteration, and destruction. Sprinklr and its Customers enter into agreements requiring that Sprinklr use the highest industry standards with respect to storage of data and the security of its system.

37.The above clauses indicate that there are sufficient protections with respect to any data that the third respondent may have access to. It not only gives the Government, as opposed to the third respondent, full control and right over the data of the people, but also obligates the third respondent to take appropriate measures to protect such data. There is a prohibition on the third respondent for using the data for purposes other than for the need intended and from sharing it with third parties without consent. It is also envisaged that no data will be available to the third respondent after the termination of the agreement. Hence, there are adequate protections to ensure that there is no possibility of any misuse or commercialization of the data by the third respondent. In any event, the Petitioner has not given any details of how this data can possibly be misused or commercialized or which information provided is sensitive or infringes the right to privacy. As such, mere baseless apprehension of misuse of data, without anything more, is not sufficient reason to entertain the present Petition.

DATA PROTECTION

38.Data needs to be protected from unauthorised access and usage non specified purposes. The issue of data protection is to be considered under 3 phases.

A. **Data protection during Transit**: The Secure Socket Layer (SSL) is used, which is the industry standard

B. **Data protection during Storage**: Ministry of Electronics and Information Technology (MIETY), Government of India, has empanelled 12 Cloud providers and Amazon is one of the Empanelled Cloud providers. All Government empanelled Cloud Providers are audited by Standardisation Testing and Quality Certification (STQC) Directorate, attached to MIETY, and is made sure that all data are stored in India, specifically Government Data.. All such Cloud Providers have signed Non Disclosure Agreements with the Government of India. Any State Government or local government can

host their applications in MIETY empanelled Cloud Providers, as they are already MEITY and STQC audited.

Guidelines for Government Departments on Contractual Terms Related to Cloud Services, allows storage of sensitive information

> "b. Privacy and Security Safeguards.
>
> The Department may ensure that specific clauses pertaining to the following are included in to the contracts.
>
> i. If the data is classified as very sensitive, the Departments may include a clause to ensure that the data is encrypted as part of a standard security process for highly sensitive content or choose the right cryptographic algorithms evaluating security, performance, and compliance requirements specific to their application and may choose from multiple key management options."

C. <u>Data Protection during processing</u>

The Software as a Service (SAAS) provided by the third respondent analyses the unstructured data stored in the CLOUD and converts it into a structured one. The Order form and Master Service agreement, together with the Service level Agreement and Data protection addendum provides for security of the data while processing. The privacy policy of the company and the international data protection norms (including the General Data Protection Regulations) ensures a high level of confidence. Further, the cloud service provider will provide the logs for audit and through frequent audit any possibility of unintended use is traceable and corrected. The instance of the application has been created in the CDIT account and data is also residing in the CDIT account. The technology transfer is in process to enable the Government entity to take over the processing internally.

AS TO WHY THE SOFTWARE AS A SERVICE OF THE THIRD RESPONDENT IS NECESSARY

39. The software as a service now provided by the third respondent is essential for Kerala, as a manual or semi-digital system, which is in force at present, will become ineffective with a rapid rise in the number of positive COVID-19 cases or with large increase in the number of persons to be put under quarantine. The platform made available by the third respondent can handle large volumes of multi channel data which will facilitate effective home monitoring as it can capture the entries on the condition of the person under observation.

40. The only way to contain the spread of COVID is to cut off the ways it could spread from one person to another. Therefore, the strategy being followed by the State of Kerala is unique, where all the suspected cases are kept under monitored home isolation. However, every person under home isolation is treated as if the person is under a supervised quarantine through a system of daily visits by authorised persons. This strategy ensures that the hospital beds are not occupied unnecessarily and at the same time the system of monitoring through daily home visit safeguards the chances of missing any person if they become symptomatic.

41. The daily monitoring gathers information whether the person under observation is having a fever or other symptoms that is worsening, persisting or going down. If it is going down, it is a good sign as it may be a case of a normal flu or probably person has developed immunity to virus, even if he has been infected by COVID. But if the symptoms are persisting or worsening, those cases will require close attention. More serious is the case of persisting or worsening symptoms if the person is otherwise with less immunity. Mortality rate in such cases are high and such cases need to be attended very fast. It is for analysing this purpose, the question regarding co morbidity conditions are included. (Question No.17 in Form 5).

42. Thus, the present home surveillance system, which as adapted by the first Respondent is non-intrusive and proportionate, observes two aspects:

Is any of the people under surveillance turning symptomatic? (Question No. 15, Form 5).

Is the incidence of COVID impacting/ aggravating the existing disease conditions like cardiac problems or ailments of Kidney/ Liver or cancer (Question No. 17 Form 5).

43. The above information needs to be gathered and analysed very fast so that the medical aid can be mobilised emergently to assist the person turning to an increased risk status. When there are roughly two lakh people under surveillance, this can be done manually or with a minimally powerful database. But in a situation where large number of persons like most of the elderly and a good number of NCD patients are to be kept under surveillance, the manual or semi-digitalised system would not stand a chance. It is in such a condition that the services of the third respondent, which can provide these types of reports instantaneously, will come to full action.

44. As per the Kerala Economic Review 2019, there are 42,27,879 elderly people (above 60 years of age) in the State. This, along with NCD patients, put together will constitute approximately 50 Lakhs persons who need to be under monitoring. The NRKs likely to be returning to the State and going under surveillance would add another 5-10 lakhs persons. More than that, by any unfortunate circumstances, if there is a community spread of the disease the number of persons under surveillance would leap up to 120 - 180 lakhs. These large numbers can be managed effectively only using a Big Data analytics team and that is the significance of positioning the third respondent's system. It is also proposed that with the user friendly interface, this system can convert all such surveillance/ home isolation monitoring cases as can be done in a self-reporting mode. This will save the effort of volunteers or officials from daily visits to homes, which may turn to be tedious and unpractical

if the numbers grow up exponentially. More over in a scenario of higher incidence of epidemic or a community spread, volunteers and officials will be reluctant to undertake home visits (and it will be unsafe to send them too), the automated system of the third respondent will turn out to be the most effective support mechanism to save many valuable lives.

IS NOT THE INFORMATION TECHNOLOGY (IT) DEPARTMENT OF THE STATE EQUIPPED TO CARRY OUT THE FUNCTIONS THAT IS BEING CARRIED OUT THROUGH THE THIRD RESPONDENT?

45. Epidemiological prediction models are still evolving, in the context of a pandemic like COVID-19. While some of the models have been validated, others are still at various stages of research. However, predictions from different learned institutions had indicated that the COVID19 pandemic could potentially affect a very large segment of the society and the number of persons under surveillance and confirmed positive cases could surge exponentially within very short duration. As per the early projections, the data to be compiled and processed would be huge and the time available for development of software for doing this was very short.

46. None of the Government Institutions in Kerala are presently capable of doing big data analysis, particularly big data analytics with unstructured data, or to offer solutions in the shortest possible time, that the above situation would demand. In addition to the ability to do big data analytics at an advanced level, the agency chosen would have to have the capacity to dynamically respond to various predictions and different sets of parameters thrown up by the evolving epidemiological models. Furthermore, such an agency would also have to have the capability to integrate data from multiple sources, within minimal response times.

47. Undertaking a capacity building programme and enabling the available Government Institutions to manage the task at hand would take time and effort, which could not be spared at the time of a pandemic. Besides the risk of not being able to arrive at a reliable and robust solution quickly,

even after such efforts are initiated, will amount to putting the life and safety of the people of the State at danger and could jeopardise and compromise public interest irreparably.

48. In the field of big data, it is experience that counts first and foremost, especially in a situation which calls for rapid response to save the lives of the people of the State. Hence, it is not practical or effective to get the Government Institutions prepared adequately in a reasonably quick period to carry out the task in a very short duration and take up such a daunting challenge.

49. Since it was not practically possible to manage the task by using the available resources with the IT Department, the straight forward and logical way out was to identify a solution which has already been proved to be suitable for big data analytics and which could be made available and customised for addressing the problem at hand within the shortest possible time.

WHY THIS MUCH BIG DATA ANALYSIS IS REQUIRED WHEN THE NUMBER OF AFFECTED PERSONS IS GETTING LOW DAY BY DAY?

50. It is too early to conclude that the worst phase of COVID 19 pandemic is over. Any sense of complacency will prove dangerous and incalculably costly to the State. The real figures will be known only after the lockdown is lifted and international and domestic flights and trains are allowed, when we expect lakhs of people from other countries and states, including from the badly affected places, to return to India. In fact, at this juncture, Kerala has to recognize and prepare for handling a set of triple issues namely- (1). Another phase of COVID-19 out-break, when boundaries are opened, lock down relaxed and the Keralites from other States and abroad start reaching back (2). Seasonal infections during rains, like fevers, flu etc. (3). Possibility of the repeat of the havoc wreaked by rain havoc like that wrecked in the State in the past two years Thus, it would be wrong and premature to judge that the issues have tided over and the incidence of infections are going down or

that the pandemic has abated. The situation does not call for any such reassurance or allow us to sit back. Caution is most vital given the situation in India and the experience of other countries. If the transition of number of cases occurred in the last 42 days is observed, it can be understood that the reduction happened consecutively only for two days, and this trend reversed the very next day.

51. The lessons from elsewhere also substantiates the same inference. For example, in the case of Singapore, the first case was detected on January 23, 2020. Singapore aggressively tracked positive cases, tested extensively and until March 10, 2020 and as a result their curve had flattened considerably with total number of cases less than 100. So for a while, the pandemic situation in Singapore seemed to be under control considering that the total number of cases was around 900 at the beginning of the month. But the situation changed drastically in the last 2 weeks with more than 6000 new cases raising the total to 8000+ which is quiet high for a relatively small population of around 50 lakhs. Number of cases reported on April 20, 2020, on a single day, was more than 1400. Similar pattern can be seen in Mumbai too. Kerala and Maharashtra had similar number of cases until the 1st of April 2020. But presently, Maharashtra is witnessing an explosion with 500+ cases being reporting daily.

52. Even if the situation is effectively managed, that has to be dealt with in the wake of large scale influx of people into the State, many experts concur that the pandemic is going to remain in the community until a certain percentage of the people are infected (so that herd immunity develops and transmission stops by itself) or until we find a cure or vaccine for the virus. It is quite difficult even to hazard a guess on how long this could take. It could even take several months before that could happen. Hence, it will be suicidal to think that the flattening of the curve of epidemic incidence has stabilised and that the incidence of the epidemic is going to necessarily remain like this, once the lock down restrictions are relaxed. Hence, it is imperative to keep vigil for an extended period, so that the people of the State are protected to the best

of Government's ability and that the vulnerable population in the State is kept away and adequately insulated from the infection as far as possible. It is only in public interest that the Government should be vigilant and ready to manage the situation in case it takes a turn for the worse.

53. As stated above, the number of people which was projected to be affected by COVID 19 was huge and hence big data analytics will be necessary to be applied for effectively handling this large data size. It is in this situation, the software which has been used for large data sets was identified and procured in 'Software as a service' (SaaS) mode.

54. Moreover, it is also expected that there will be multiple communication channels including social media to collect the data, making it a combination of structured and unstructured data. There could also be data coming in multiple languages. This requires powerful software which can collate such disjointed data sets and come out with meaningful analysis. The third respondent's service was procured for this purpose as building such software would require a lot of significant resources and time, which was not available with the IT Department internally. It is also pertinent to note that when designing large software, both Government of India and Government of Kerala have depended on third party products as in the case of Passport Seva Kendras, Kerala E-Health project etc.

AS REGARDS THE JURISDICTION OF NEW YORK COURTS

55. The primary concern that appears to be raised in a preemptive manner in the above Petition appears to be the apprehension of possible misuse by third Respondent of the data being collected and processed. This apprehension has also resulted in a query on data principals being able to initiate penal actions for data breaches.

56. Firstly, the choice of jurisdiction i.e., of New York Courts, is a standard form contract of third Respondent. The first Respondent has negotiated a very viable agreement ensuring both legal and technical security of the data being collected and processed. The said data resides in India on cloud services duly approved by the second Respondent. Any data

breach or even apprehension thereof therefore pertains to occurrences in India. The Agreement containing the mandate for New York jurisdiction is solely with respect to breach of the terms of the contract by parties thereto. These terms have been agreed keeping the best interests of the State i.e., its urgent need for effective Information Technology tools to combat the pandemic and it has chosen the best possible *pro bono* option. The term of this engagement is also for a very limited period with expansive exit options and protective measures. The data principals not being party to the same, these terms do not bind them.

57. Further, the apprehension raised is for initiation of penal actions for breach. These penal actions would fall within the purview of the IT Act, which provides for several penal actions against third Respondent, which would also be an "intermediary" including the mandate for compulsory reporting of a data breach. In such instances it is open not only for data principals but also the first Respondent Government of Kerala to initiate action in India, as a restriction on jurisdiction for civil action does not limit Criminal prosecutions or jurisdictions therefor.

58. It is pertinent that data resides in India and hence there would no issues of jurisdiction. Even if any breach occurs from outside India, S.75 of the IT Act empowers initiation of prosecution within India provided such breach impacts a computer or computer resource within India.

59. Section 75 of the IT providing for jurisdiction for Indian courts for all IT assets residing in India, is extracted hereunder

> Section 75: Act to apply for offence or contravention committed outside India:
>
> (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
>
> (2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any

> person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

60. This section has broader perspective including cyber-crime, committed by cyber criminals. Since the Data is localized (kept in the Amazon Web Services (AWS) servers in India) all the laws of protection of data in the country is applicable to this arrangement with the third respondent and any breach shall come under the purview of section 75 of the Indian IT act. Further additional claims on data breach and agreement violation only need be and can be addressed through the courts of New York State.

61. Guidelines for Government Departments on Contractual Terms Related to Cloud Services, under clause 2.1 (f), covers the provision for law enforcement agency to intervene.

> "(f). Law Enforcement Request: The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the Service Provider to perform all due diligence before releasing any such information to any such law enforcement agency."

62. The decision to accept standard form contract in the light of the emergency faced is a subjective governance decision of the first Respondent and the Petitioner questioning the same appears to be misconceived and untenable. Neither the choice of the third Respondent nor of jurisdiction for civil disputes *inter se* parties is excessive or unsustainable in the light of legitimate State aim and the interests of the citizens and residents of the State of Kerala.

REGARDING THE ALLEGATIONS THAT THE LAW DEPARTMENT WAS BYPASSED

63. The action taken in engaging the third respondent tantamount to issue of a Purchase Order to avail the service of a readymade software application, with the set of conditions binding to the purchase that accompany it. The head of the Administrative Department has the full authorisation for issuance of a purchase order for goods or services with price less than Rs15,000/- . In this case the service is offered on probono basis and hence there is no cost involved i.e. the cost involved is zero. None of the rules or procedures in Government necessitates that the Purchase Order being issued by an Administrative Department for the purchase of any product or service, is to be scrutinised by the Law Department. Hence, this is not bypassing of Law Department and the matter did not require any consultation with the said Department at all.

POINTS OF LAW TO BE URGED

64. The Government has taken every earnest attempt to see that the data collected is protected. The purchase order, coupled with incidental agreement, is intended to prevent any misuse of such data. The Government, in the present crisis situation, is compelled to collect the data and get it structured through an Information Technology Platform. That use of Information Technology is the best option to combat this crisis threatening humankind, is affirmed by the Petitioner himself in his Petition. It is trite and settled law that the fundamental right to privacy is subject to limitations and reasonable restrictions; that privacy is not an absolute right; that the right to privacy is subservient to and must bow down to compelling State interest; and that it is susceptible to invasion if it meets the three fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate State aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.

65. The DM Act enables the State Government to take recourse to measures, as it deems necessary or expedient, for the purpose of disaster management, for prevention of disasters, mitigation, preparedness and

capacity building and for the purpose of securing effective implementation of provisions of the said Act. The provisions of the 2020 Ordinance empower the Government to take recourse to measures as may be necessary for the regulation and prevention of epidemic diseases and protect actions taken in good faith by the Government. The information sought for by the Government is expedient for the prevention of spreading of COVID 19 and for enhancing the preparedness to meet the situation arising of the spread of the pandemic. The Petitioner himself in the Writ Petition has commended the Government for the actions it has taken to prevent the spread of the pandemic. In fact, in paragraph 6 of the Petition, it is admitted that the decision was taken collectively by a team of experts. It is submitted that the COVID-19 pandemic has resulted in a situation of emergency which is being compared to a war-like circumstance by many experts. In such a situation, urgent policy decisions have to be taken by the democratically elected Government in its executive capacity in the interest of public health and public interest, and it must be given a greater free play in the joints so that it is better able to perform its functions. Policy decisions taken by the executive in such a dire situation with the help of experts cannot be said to be arbitrary or subjected to the same level of scrutiny as in ordinary times, as long as the action was necessary and proportionate to achieve the intended purpose.

66. As stated above, the information being collected is to examine the vulnerability of different parts of the State to different forms of disasters and specify measures to be taken for their prevention or mitigation; to lay down guidelines for preparation of disaster management plans by the departments of the Government of the State and the District Authorities; to provide shelter, food, drinking water, essential provisions, healthcare and services in accordance with the standards laid down by the National Disaster Management Authority and State Disaster Management Authority; to inspect the persons arriving in the State by air, rail, road, sea or any other means or in quarantine or in isolation, as the case may be, in hospital, temporary accommodation, home or otherwise of persons suspected of being infected with any such disease by the officers

authorized in the regulation or orders; and to coordinate and monitor the implementation of the National Policy, the National Plan and the State Plan. The information is being collected to protect the life of the informant/ data principal as well as lives of numerous others and in the interest of public health.

67. The legitimate aim of the first respondent State is to control the spread of COVID -19 pandemic. The Government, under the guidance of experts, has decided on the course of action for the same. Such course of action includes quarantining of the infected persons and primary and secondary contacts of such persons. Such course of action also includes reverse quarantine of identified vulnerable sections of the society. The State has to cater to the needs of such quarantined persons. The State has to chalk out its strategy to combat the pandemic, which has affected the entire world at large. The State's endeavour is to save the lives of its residents. The minimum information collected by the State for the same and the streamlining of such data with the product of the third respondent cannot be said to be infraction of the right to privacy of the writ petitioner or any other person, particularly when such collection of data and streamlining of the same is for the purposes mandated by the DM Act and the 2020 Ordinance. When the lives of millions are at stakes, the privacy rights, if any of the individuals, have to be subservient to the same.

68. In the current situation of emergency, it is necessary to balance the public right life and health as against the right to privacy of individuals. Given the highly contagious nature of the disease and its exponential growth rate and high mortality rate, it is impossible to combat the disease without adequate data. There is not only lack of time to obtain consent from individuals but also, if some people give consent and others refuse to give consent, it is impossible to have a complete picture of the spread of the disease and the possible path it may take, rendering the entire exercise infructuous. No choice can be given to individuals in such exigency when the right to health of the society at large is at stake, and the Government has to be permitted to take a decision in the interest

of the entire public before it is too late. Such information will only be used for the collective benefit of the public, and not to the prejudice of any individual. Pertinently, such data is not being disclosed to the public at large, but to a third party for a limited purpose which the Government is unable to undertake at this stage and for a limited duration. This cannot be termed as an unreasonable interference in a person's right to privacy.

69. The decision of the 9 Judge Bench of the Hon'ble Supreme Court in KS Puttaswamy v. Union of India, (2017) 10 SCC 1, itself held that reasonable restrictions can be imposed on the right to privacy in view of compelling State interest or public health. In Mr. X v. Hospital Z, (1998) 8 SCC 296, where the disclosure of Mr. X's HIV+ status to his fiancée was under challenge inter alia for violating his right to privacy, the Hon'ble Supreme Court held as follows:

"Ms 'Y', with whom the marriage of the appellant was settled, was saved in time by the disclosure of the vital information that the appellant was HIV(+). The disease which is communicable would have been positively communicated to her immediately on the consummation of marriage. As a human being, Ms 'Y' must also enjoy, as she obviously is entitled to, all the Human Rights available to any other human being. This is apart from, and in addition to, the Fundamental Right available to her under Article 21, which, as we have seen, guarantees "right to life" to every citizen of this country. This right would positively include the right to be told that a person, with whom she was proposed to be married, was the victim of a deadly disease, which was sexually communicable. Since "right to life" includes right to lead a healthy life so as to enjoy all the faculties of the human body in their prime condition, the respondents, by their disclosure that the appellant was HIV(+), cannot be said to have, in any way, either violated the rule of confidentiality or the right of privacy. Moreover, where there is a clash of two Fundamental Rights, as in the instant case, namely, the appellant's right to privacy as part of right to life and Ms 'Y's right to lead a healthy life which is her Fundamental Right under Article 21, the right which would advance

the public morality or public interest, would alone be enforced through the process of court, for the reason that moral considerations cannot be kept at bay and the Judges are not expected to sit as mute structures of clay in the hall known as the courtroom, but have to be sensitive, "in the sense that they must keep their fingers firmly upon the pulse of the accepted morality of the day". (See: Allen: Legal Duties)"

Similarly, in the present case also, the right to health of the people and public interest in controlling an epidemic would take precedence over the right to privacy. The measure therefore bears a rational nexus to the purpose it seeks to achieve and satisfies the test of proportionality.

70. Article 47 of the Constitution of India mandates the State to have regard to the improvement of public health as its primary duty, as has been reiterated by the Hon'ble Supreme Court in the 5 Judge Bench decision of KS Puttaswamy v.Union of India, (2019) 1 SCC 1 (para 1214). The 2020 Ordinance is a legislation framed by the State, interalia, in accordance with the mandate of Article 47 of the Constitution. DM Act, 2005 is also relatable to Article 47. Any act done by the State in implementation of a directive principle of State Policy cannot be held to be violative of Article 14 of the Constitution of India. Consequently, any collection of information or data by the State for protecting public health as well as the health of the data principal cannot be challenged on the ground of violation of Article 14 of the Constitution of India.

71. Personal Data Protection Bill, 2019 was tabled in the Loksabha on 11th December, 2019. Section 12 of the said Bill provides that the personal data can be processed by the State without consent to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual; to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health; or to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order. Similar was Section 15 of the Draft Data Protection Bill, 2018

72. Paragraph 1 of Article 9 of the Regulation (EU) 2016/679 of the European Parliament and oft Council on the Protection of Natural Persons with regard to The Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation) provides that Processing of personal data concerning health shall be prohibited. However, Paragraph 2 (i) of Articles 9 provides that Paragraph 1 shall not apply if processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats. Paragraph 46 of the Adoption Clause of the said Regulations provides that the processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person and when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread.

73. Sections 43A and 72A of the IT Act along with the Rules framed under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (hereinafter referred to as "the 2011 Rules" for short) cover the gamut of laws pertaining to personal data protection presently. These provisions are in the form of negative covenants i.e., that it mandates penalties for body corporates, which violate reasonable security practises or the Central Government Rules for collecting and processing of sensitive personal data or information

74. As per Rule 4 of the 2011 Rules, the body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf shall provide for (i) Clear and easily accessible statements of its practices and

policies; (ii) type of personal or sensitive personal data or information collected under rule 3; (iii) purpose of collection and usage of such information; (iv) disclosure of information including sensitive personal data or information as provided in Rule 6; and (v) reasonable security practices and procedures as provided under Rule 8. The third respondent has provided for a privacy policy and the same was made available to the first respondent also.

75. Rule 5 of the 2011 Rules mandates a body corporate to obtain informed consent from a provider of information and the first respondent State is not a body corporate as defined under either the IT Act or the 2011 Rules. Further, the information being sought for is required by the Government in terms for the purposes of the mandate conferred on it as per the DM Act and 2020 Ordinance to manage an epidemic.

76. The data being collected is required in the interests of the health of the data principal as well as that of the others and the society as a whole. The data collection is in pursuance of the mandate of the State as per the provisions of the DM Act and the 2020 Ordinance to manage the COVID -19 pandemic. In the said circumstances, it cannot be said that there is any violation of individual right of privacy. The effective management of COVID-19pandemic required availability of structured data in real time. In so far as the Government or Governmental agencies were not technically equipped to handle and stream line and structure such huge volume of data and on account of the time constraints, necessitated by the emergent need to curb the spread of COVID 19, the Government placed an Order with the third respondent for its product. The order was in response to the Offer of the third respondent to provide software service on zero costs during COVID – 19 time. The Government was also compelled because at that point of time, the experts were predicting that one-fourth of the total residents of the State were going to be affected with COVID. The third respondent is also a pro bono participant with the World Health Organisation in developing its dash board for providing COVID – 19 updates. Such an Order to the third respondent for its product does not need any concurrence at the

instance of the second respondent. The Additional Platform Product Terms of the Order Form and the clauses of the Master Service Agreement as well as the Mutual Non Disclosure Agreement provide for provisions with regard to Data Security. There is a published privacy policy for the third respondent, as mandated under the 2011 Rules. In the said circumstances, there was nothing wrong in the Government purchasing the product of the third respondent for structuring the data being collected for the purpose of abatement of the pandemic of COVID 19. The product is absolutely necessary for meeting the situation wherein the State is anticipating return of large number of expatriates, to the tune of lakhs. Any contrary measure, at this juncture, will adversely affect the COVID Management plans of the State.

77. Since certain issues were raised with regard to the arrangements made with the third respondent for extension of their software as a service, the Government appointed a two member Committee to look into the relevant aspects and to submit a report regarding the same. A true photocopy of GO (MS) No. 79/2020/ GAD dated 20/04/2020, in this regard, is produced herewith as **Annexure- R1(c)**.

78. The writ petition is devoid of merits. The writ petition is not sustainable either in law or on facts. The Petitioner himself clearly acknowledges the "commendable" job that the first Respondent is doing in containing the Covid pandemic and also an affirmation that Information Technology tools are the best option to combat this unprecedented crisis that in the words of the Petitioner is *"threatening the very existence of humankind"*. The writ petition is highly premature in so far as the writ petitioner has not made out any case of actual data misuse. The entire writ petition is wholly based on surmises and conjectures. The assumptions based on which even these conjectures have been put forth are unsubstantiated. Further, the petitioner has not provided any information to the Government nor sought for clarifications before rushing to court to stop a very important containment process initiated by the first Respondent. He is also not privy to any complaint made by anyone regarding breach of their privacy on account of any misuse of

information passed on to the Government. Any restraint or delay in deploying the Information Technology tools or methodologies being formulated by the first Respondent will materially and irreversibly harm the health, well-being and lives of citizens and residents of Kerala It is prayed that the writ petition may be dismissed inlimine.

Dated this 22nd day of April, 2020.

V.Manu

Senior Government Pleader