

**BEFORE THE HONOURABLE HIGH COURT OF KERALA AT**  
**ERNAKULAM**

**Writ Petition (Civil) No. 9498 of 2020**

**Between**

**Balu Gopalakrishnan : Petitioner**

**And**

**State of Kerala and others : Respondents**

**COUNTER AFFIDAVIT FILED FOR AND ON BEHALF OF THE FIRST  
RESPONDENT**

**V.MANU  
SENIOR GOVERNMENT PLEADER**

## APPENDIX

### Respondents' Exhibits

|    |                                |   |
|----|--------------------------------|---|
| 1  | <b><u>Exhibit – R1(a)</u></b>  | A true photocopy of the situation report dated 16/3/2020 of the World Health Organisation   |
| 2  | <b><u>Exhibit – R1 (b)</u></b> | A true photocopy of the study report dated 24/03/2020   |
| 3  | <b><u>Exhibit – R1 (c)</u></b> | True copy of GO(MS ) No. 49/2020/ ITD dated 21/04/2020  |
| 4  | <b><u>Exhibit – R1 (d)</u></b> | True copy of the work order dated 22/04/2020  |
| 5  | <b><u>Exhibit – R1 (e)</u></b> | True photocopy of the Log Analysis Report dated 23/04/2020  |
| 6  | <b><u>Exhibit R1(f)</u></b>    | True photocopy of GO (MS) No. 79/2020/ GAD dated 20/04/2020   |
| 7  | <b><u>Exhibit R1 (g)</u></b>   | True photocopy of the Letter No:- IT-B1/25/2020-ITD dated 07/05/2020 from the Principal Secretary to Government to the Director, Kerala State IT Mission, Thiruvananthapuram and the Registrar, C-DIT, Thiruvananthapuram                   |
| 8  | <b><u>Exhibit R1 (h)</u></b>   | True photocopy of the Letter No-IT-B1/25/2020-ITD-Part(3)dated 12/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department   |
| 9  | <b><u>Exhibit R1 (i)</u></b>   | True photocopy of the Letter No- IT-B1/25/2020-ITD dated 07/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Chief Executive Officer, M/s. Sprinklr Incorporation |
| 10 | <b><u>Exhibit R1 (j)</u></b>   | True photocopy of the Letter dated 14.05.2020 from M/s. Sprinklr Incorporation  |
| 11 | <b><u>Exhibit R1 (k)</u></b>   | True photocopy of the Letter No- IT-B1/25/2020-ITD dated 13/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Chief Executive Officer, M/s. Sprinklr Incorporation |

|    |                                |   |
|----|--------------------------------|---|
| 12 | <b><u>Exhibit R1 (l)</u></b>   | True photocopy of the Letter No- IT-B1/25/2020-ITD dated 16/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Chief Executive Officer, M/s. Sprinklr Incorporation           |
| 13 | <b><u>Exhibit R1 (m)</u></b>   | True photocopy of the Letter dated 29/04/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Secretary, Ministry of Electronics and Information Technology, Government of India   |
| 14 | <b><u>Exhibit R1 (n):</u></b>  | True photocopy of the Letter dated 02/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Secretary, Ministry of Electronics and Information Technology, Government of India   |
| 15 | <b><u>Exhibit R1 (o) :</u></b> | A true photocopy of the Letter dated 15/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Secretary, Ministry of Electronics and Information Technology, Government of India |
| 16 | <b><u>Exhibit R1 (p) :</u></b> | True photocopy of the Letter dated 15/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Director General, National Informatics Centre  |

Dated this the 19<sup>th</sup> day of May, 2020

V.MANU  
SENIOR GOVERNMENT PLEADER

**BEFORE THE HONOURABLE HIGH COURT OF KERALA AT  
ERNAKULAM**

**Writ Petition (Civil) No. 9498 of 2020**

**Between**

**Balu Gopalakrishnan** : Petitioner

**And**

**State of Kerala and others** : Respondents

**INDEX**

| Sl.No. | Particulars  | Page No.  |
|--------|--|-----------|
| 1      | Counter Affidavit filed for and on behalf of the first respondent  | 1 - 54    |
| 2      | <b><u>Exhibit – R1(a)</u></b> : A true photocopy of the situation report dated 16/3/2020 of the World Health Organisation  | 55 - 63   |
| 3      | <b><u>Exhibit – R1 (b)</u></b> : A true photocopy of the study report dated 24/03/2020   | 64 - 96   |
| 4      | <b><u>Exhibit – R1 (c)</u></b> : True copy of GO(MS ) No. 49/2020/ ITD dated 21/04/2020  | 97        |
| 5      | <b><u>Exhibit – R1 (d)</u></b> : True copy of the work order dated 22/04/2020  | 98        |
| 6      | <b><u>Exhibit – R1 (e)</u></b> : True photocopy of the Log Analysis Report dated 23/04/2020  | 99 – 106  |
| 7      | <b><u>Exhibit R1(f)</u></b> : True photocopy of GO (MS) No. 79/2020/ GAD dated 20/04/2020  | 107 - 108 |
| 8      | <b><u>Exhibit R1 (g)</u></b> : True photocopy of the Letter No:- IT-B1/25/2020-ITD dated 07/05/2020 from the Principal Secretary to Government to the Director, Kerala State IT Mission, Thiruvananthapuram and the Registrar, C-DIT, Thiruvananthapuram | 109       |
| 9      | <b><u>Exhibit R1 (h)</u></b> : True photocopy of the Letter No-IT-B1/25/2020-ITD-Part(3)dated12/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department  | 110 – 111 |

|    |  |           |
|----|--|-----------|
| 10 | <b><u>Exhibit R1 (i)</u></b> : True photocopy of the Letter No- IT-B1/25/2020-ITD dated 07/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Chief Executive Officer, M/s. Sprinklr Incorporation           | 112 – 113 |
| 11 | <b><u>Exhibit R1 (j)</u></b> : True photocopy of the Letter dated 14.05.2020 from M/s. Sprinklr Incorporation  | 114 – 116 |
| 12 | <b><u>Exhibit R1 (k)</u></b> : True photocopy of the Letter No- IT-B1/25/2020-ITD dated 13/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Chief Executive Officer, M/s. Sprinklr Incorporation           | 117       |
| 13 | <b><u>Exhibit R1 (l)</u></b> : True photocopy of the Letter No- IT-B1/25/2020-ITD dated 16/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Chief Executive Officer, M/s. Sprinklr Incorporation           | 118       |
| 14 | <b><u>Exhibit R1 (m)</u></b> : True photocopy of the Letter dated 29/04/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Secretary, Ministry of Electronics and Information Technology, Government of India   | 119 – 120 |
| 15 | <b><u>Exhibit R1 (n)</u></b> : True photocopy of the Letter dated 02/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Secretary, Ministry of Electronics and Information Technology, Government of India   | 121 – 122 |
| 16 | <b><u>Exhibit R1 (o)</u></b> : A true photocopy of the Letter dated 15/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Secretary, Ministry of Electronics and Information Technology, Government of India | 123       |
| 17 | <b><u>Exhibit R1 (p)</u></b> : True photocopy of the Letter dated 15/05/2020 of the Principal Secretary to Government of Kerala, Electronics and IT (B) Department, Government of Kerala to the Director General, National Informatics Centre  | 124       |

Dated this the 19<sup>th</sup> day of May 2020

V.MANU  
SENIOR GOVERNMENT PLEADER

**BEFORE THE HONOURABLE HIGH COURT OF KERALA AT**  
**ERNAKULAM**

**Writ Petition (Civil) No. 9498 of 2020**

**Between**

**Balu Gopalakrishnan : Petitioner**

**And**

**State of Kerala and others : Respondents**

**COUNTER AFFIDAVIT FILED FOR AND ON BEHALF OF THE FIRST**  
**RESPONDENT**

I, Vinod.G, S/o Gangadharan.S, aged 47 years, residing at Thiruvananthapuram and now at Ernakulam do hereby solemnly affirm and state as follows:

1. I am the Joint Secretary, Information Technology (B) Department, Government of Kerala. I am conversant with the facts of the case, as revealed from the relevant files, and am competent to swear to this affidavit. I am swearing to this affidavit for and on behalf of the first respondent, for which I am duly authorised.
2. The aforementioned writ petition has been filed impugning the purchase by the first respondent of the Software as a Service (herein referred to as “the SaaS” for short) from the third respondent (“Sprinklr”). This counter affidavit, though deals with the averments and allegations in the aforementioned writ petition in its entirety, is not filed by way of parawise counter. Absence of specific denials shall not amount to admission of all or any of the allegations and contentions in the Petition and, unless specifically admitted, all such allegations and contentions are denied as false, baseless, untenable and unsustainable. This counter affidavit also deals with the averments and allegations in the following writ petitions, on identical subject matter and raising similar contentions and reliefs, namely Writ Petitions (Civil) numbered 9530 (filed by Shri. K.Surendran), 9531 (filed by Shri. Mathew Varghese), 9532 (filed by Shri. Binosh Alex Bruce) and 9540 (filed by Shri. Ramesh Chennithala), all of the

year 2020. It is most humbly submitted that this counter affidavit will be adopted in all the said writ petitions with copies duly served.

3. All the averments in the said writ petitions, save those that are expressly admitted or otherwise traversed hereunder, are denied. The said writ petitions are neither maintainable in law nor on facts.
4. A detailed statement dated 22/04/2020 and an additional statement dated 24/04/2020 were filed on behalf of the first respondent in Writ Petition (Civil) No. 9498 of 2020 (then Writ Petition (Civil) Temporary No. 84 of 2020). The averments in the said statements may also be treated as part of this counter affidavit. The averments in this counter affidavit may be treated along with and in continuation of the averments in the said statements. The said statements were filed in the limited available time of two days, that too amidst COVID lock down with rigorous regulations, with the minimum information that could be collected, solely for the purpose of admission hearing of the Writ Petitions (Civil) now numbered as 9498, 9530, 9531, 9532 and 9540 of 2020. It is therefore that this detailed counter affidavit is being filed.
5. The averments, allegations and contentions in Writ Petition (Civil) No. 9498 of 2020 (filed by Shri. Balu Gopalakrishnan) to the effect that the State was taking illegal measures to transfer sensitive medical information to a third party entity, which was a clear misuse and exercise of arbitrary power of the State; that though it was stated on behalf of the first Respondent that the data was now being transferred to a Government of Kerala website and not to that of the third respondent, the data was still getting transferred to the third Respondent's server; that the landing server still belonged to the third Respondent and the url "housevisit.kerala.gov.in" was just a façade; that the actions of the first Respondent were in clear violation of the provisions of the Information Technology Act, 2000 (hereinafter referred to as "the IT Act" for short), which provided for securing sensitive information and the manner in which it could be transmitted; that the contract, entered into in a haphazard manner, exposed the information of common laymen into the hands of a private entity; that the second Respondent, the authority which should concur with such decisions of the State, ought to have been consulted before executing the alleged agreement and their concurrence sought for; and that the data which was aggregated and supplied to the third Respondent was a valuable commodity in the data market

which could fetch millions of dollars, are all wrong, baseless and unfounded, and hence denied. The averments, allegations and contentions regarding there being lack of purported informed consent and that the State could not harp upon a case of implied consent of the data principal, are not sustainable in law. The contention that the act of the first respondent impinged upon the fundamental rights guaranteed under Articles 14 and 21 of the Constitution of India, is also not sustainable in law. It is also incorrect that the acts of the Government of Kerala in any manner, violates the provisions of the IT Act. The similar and other contentions, averments and allegations in the said writ petition are also wrong and hence denied.

6. The averments, allegations and contentions in Writ Petition (Civil) No. 9530 of 2020 (filed by Shri. K.Surendran) to the effect that the arrangement with Sprinklr impinged upon the fundamental right guaranteed to the data principals under Article 21 of the Constitution of India; that the sharing of data with Sprinklr would affect national security interests; that the terms and conditions of the Master Services Agreement would lead to corruption and financial loss to the exchequer as well as cause misappropriation of the State Fund; that the clauses of the said agreement only protected the interests of Sprinklr; that there was violation of the provisions contemplated under Articles 298, 299 and 300 of the Constitution of India; that there was every possibility of the data being misused, attracting offences under Sections 65, 66, 67, 71, 72 and 74 of the IT Act, apart from those under Sections 463 to 471 of the Penal Code; that if Sprinklr made illegal profit out of the said data, the same would amount to offences under Sections 7, 8, 9, 10, 11 and 12 of the Prevention of Corruption Act (hereinafter referred to as “the PC Act: for short); that clause .6 of the Master Service Agreement violated the interest of the State; that clause 7 of the same only protected the interests of Sprinklr; that clause 8 therein was highly unethical and violative of Article 21 of the Constitution of India; that clause 10 therein was against the provisions of Article 298 and 300 of the Constitution of India; that the acceptance of a foreign jurisdiction without following necessary legal vetting was illegal and unconstitutional; that the mode and way of entering into a business contract and that the background for entering the Master Services Agreement was hidden and all the procedures for the same being fraudulently created, are all patently false, baseless, unsubstantiated and

unfounded and hence denied. The similar and other contentions, averments and allegations in the said writ petition are also wrong.

7. The cause of action for filing Writ Petition (Civil) No. 9531 of 2020 (filed by Shri. Mathew Varghese), going by the pleadings therein, stems from the allegations of the various political leaders, which purported allegations have been reduced in paragraph 14 of the said writ petition. The allegations in paragraph 14 of the said writ petition are false and hence denied. The averments, allegations and contentions to the effect that the value of the data procured could be quantified at Rupees 200 Crores; that the engagement of Sprinklr, purportedly keeping everyone, including the relevant Departments in darkness, amounted to a corrupt practice within the meaning of Section 13 of the PC Act; that the explanation that the services of Sprinklr was free was a naive one in so far as the data supplied to it was of the value of Rupees 200 Crores; and that the deal with Sprinklr, on the face of it, gave an impression that the allegations of the Leader of Opposition (such allegation, as referred to by the said writ petitioner, are ex facie defamatory and wrong and hence not quoted herein) were true; are all wrong, speculative, completely baseless and unfounded and hence denied. The other and similar allegations and averments in the said writ petition are also denied.
8. The averments, allegations and contentions in Writ Petition (Civil) No. 9532 of 2020 (filed by Shri. Binosh Alex Bruce) to the effect that the infrastructure for data collection was inadequate and unsafe; that there were no required controls for data protection; that there was no mention of applications used by the administrators and the security aspect of such applications; that multi factor authentication was required; that there was no details pertaining to storage and encryption of data back up; that if Sprinklr allowed administration from personal devices, there was a risk of data corruption and data leakage; that no details regarding the support provided by Sprinklr and Amazon to investigate any data leakage was forthcoming; that there was no restriction on copying and sharing personal data – even after removing personal identifiable information; that it was to be ascertained that Amazon and Sprinklr had carried out the background verification of all the staff who have access to data; and that there was no guarantee that the data would be encrypted and that the fourth respondent could not ensure that the data would be safe with Amazon, are all

unsustainable in law. The other and similar allegations, contentions and averments in the said writ petition are baseless, unfounded, misconceived and also unsustainable in law.

9. The averments, allegations and contentions in Writ Petition (Civil) No. 9540 of 2020 (filed by Shri. Ramesh Chennithala) to the effect that the relevant Government Order did not reveal the need for such data collection and the purpose for which it would be utilised; that the act of the Secretary of the Information Technology Department, in engaging Sprinklr , was beyond the power and authority vested on him; that no date was given in the Mutual Non Disclosure Agreement, presumably due to well known reasons; that no authorisation was given the Council of Ministers or by the concerned Departments to the Secretary of the Information Technology Department to enter into such a contract; and that there was violation of the provisions of Article 299 of the Constitution of India; are wrong, misconceived, untenable and hence denied. The allegations of malafides against eo nomine parties are based on mere surmises and conjectures and not on any cogent materials. The other and similar allegations, contentions and averments in the said writ petition are also denied.

10. It is humbly submitted that all of the abovementioned Writ Petitions are not maintainable and ought to have been rejected at the threshold and hence the issue of maintainability of the Writ Petitions ought to be taken up as a preliminary issue and decided at the outset. It is submitted that each of the above Writ Petitions are based on apprehensions, baseless and unfounded allegations, speculative conjectures and surmises and in some instances with vested interest. It is submitted that the efforts of the Government of Kerala have been commended globally, including by the Petitioner himself, and it is a matter of fact that the efforts undertaken by the said Government, in its fight against COVID19, have been exemplary. The first Respondent respects privacy of its citizens and therefore adapted one of the least intrusive methodology for collection of data of those persons in isolation. There was, therefore, a conscious effort to limit the persons and the kind of data that was being collected and the first Respondent had taken all measures to ensure its safety and security. Entertaining the vexatious filings, as above not only dilutes the exemplary initiatives of the first Respondent, but may also result in

jeopardizing the health and well - being of the citizens and residents of the State, for whose benefits all actions have been undertaken in good faith based on necessity and as deemed fit and proper by the first Respondent.

11. It is humbly submitted that if the allegations in each of the Petitions, set out above, were to be taken in their entirety, they do not make out any specific cause of action to sustain the Petitions and the only basis for these, in some instances vexatious proceedings, are mere apprehensions of the Petitioners apart from the baseless, false and unsubstantiated speculative and conjectural accusations. The Petitioner in the first Writ Petition himself admits that need for use of technology enabled tools to combat this evil of Covid19 and it is apparent that the actions of the first Respondent were relevant and appropriate. It is humbly submitted that it is a settled position that such apprehension cannot form the basis for intervention of this Hon'ble Court and the proceedings ought to be rejected at the outset on this ground alone.

12. It is further submitted that the actions taken by the first Respondent are for a legitimate State aim and proportionate and commensurate with the evil it was combating. Reasonable restrictions on privacy to check the spread of this evil i.e., COVID19 are constitutionally sustainable. It is submitted that it is within the judgment of the executive to decide on policies and methodologies and the review thereof is very limited and not substitution of the subjective satisfaction based whereon such decisions were taken. It is submitted that the grounds raised and the reliefs sought in the above Petitions are premature, misconceived and not maintainable and all Petitions ought to be rejected forthwith with costs, especially for such of those Petitions raising malicious and vexatious false claims.

13. The following submissions on facts are made without prejudice to the rights and contentions of the first Respondent herein above, and in particular with respect to the maintainability of all the Writ Petitions under response.

**FACT SITUATION WHICH NECESSITATED THE COURSE OF ACTION NOW ADOPTED BY THE STATE OF KERALA**

14. 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 the 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. As a matter of fact, there has been an instance in the State wherein 13 persons got infected from a single point contact. 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 presently known to contain the disease is to keep away from one another.

15. Ever since the first COVID – 19 case was reported, the State of Kerala took all steps to ensure proper identification of persons affected, their primary and secondary contacts and those who were 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.

16. 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.

17. 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,

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

18.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.

19. 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.

20.The Government 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. By doing so, the Government has ensured reasonable measures that are needed for the benefit of public. 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.

21.The first case of COVID19 in India was reported on 30<sup>th</sup> January, 2020, originating from China. As of 26<sup>th</sup> 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 **Exhibit – R1(a)**.

22.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 **Exhibit – R1 (b)**.

23.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 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.

24. 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.
25. 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.

26. 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/ SaaS. 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 as 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 could have turned to be fatal, if the spurt of the disease happened to be as predicted.

27. 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 implement fast. It is a data analytics company with capability of processing large volumes of data. Its 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

28. 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 the third respondent is also a pro bono partner of the World Health Organisation in developing its COVID -19 Update dash board. There was no other nexus or reason for engaging third Respondent, save and except for the circumstances set out above

29.The decision for the procurement of the SaaS application, deployed and developed by Sprinklr, the third respondent, was not a single-handed decision of the Principal Secretary of the Electronics and Information Technology Department (hereinafter referred to as the “E & IT Department” for short). The decision was taken based on clear consultations and scrutiny within the E&IT Department of the State in a committee –the IT Support Team- comprising of the heads of all institutions under the Department as well as representatives of Health Department and Local Self Government Department and State Disaster Management Authority (SDMA). The IT Support Team was formed within the Department to take forward the necessary interventions with regard to supporting COVID 19 control activities during lockdown period when the Department Sections were not in the fully functional mode. Secretaries of the Departments such as Health and Local Self Government and SDMA also attended some of the meetings and outlined their field level requirements and identified suitable officers from the respective departments for attending the regular meetings of the IT Support Team for working out the requirements in greater granularity. The team had made detailed scrutiny of the documents and technical aspects of the SaaS application and submitted the recommendations in affirmative to the Principal Secretary, E&IT Department for taking forward the matter. Hence, the actions taken by the Principal Secretary, E&IT Department to sign the document and avail the SaaS application had sufficient scrutiny and consensus on technical and functional requirements being met.

**DETAILS AND NATURE OF DATA WHICH WERE COLLECTED  
AND THE NECESSITY FOR COLLECTION OF SUCH DATA**

30.It is submitted that the details set out hereunder are without prejudice to the averments and contentions on maintainability raised herein above including the ground that the decision for such collection is rational, necessary, proportionate and reasonable. Such actions are not just of the first Respondent but across India and in fact global and in this context, the first Respondent has ensured and adapted the least intrusive mode and method of collection of data.

31.There were five types of data collected, for which there were 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

32.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, did not have a choice, is patently incorrect and misleading. As set out above, the online submissions were through a voluntary self - reporting process.

33.The data, numbered as the fifth, was collected by health workers when they visited homes to observe people in quarantine. The data collected through Form 5 (house visit form) was intended to identify any COVID related symptoms from among those under surveillance, so that the local self government could take note of that and could act immediately through the Public Health Centres; and to identify if any vulnerable citizens were there at the houses where citizens were undergoing home isolation, as they could be instructed to be under strict reverse quarantine measures. Information regarding medication being taken for other co morbidity illnesses such as blood pressure, diabetes etc was collected because it was empirically established that the virus had a high mortality rate amongst persons with such pre-existing diseases. The information was, therefore, relevant for curbing spread of the disease and also for ensuring that medical care reached the persons who were most susceptible to the disease. The information was 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 was used to collect data only from people in isolation who had high vulnerability for COVID19, so that the collection of this data was extremely essential for preventing the spread of the epidemic as well as to support the Government's effort to control the epidemic. This form collected physically

was not within the purview of the IT Act at the stage of collection. The said process was also undertaken as a process of governance by the State.

34. 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 was an essential step the Government was required to take in public interest. The data fields therein, interalia, included the following:

- Name, age , District, Panchayath, Ward and details of persons who were isolated ( not COVID patients)
- Details of travel to other countries
- Any symptoms in the isolated persons (critical for ensuring testing)
- Presence of old age persons in the house to ensure medicines.
- Any patient who was not getting medicines. (yes/No)
- 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)
- Details of any quarantine breach and travel. (ensure quarantine for containment)
- Any unusual occurrences in the community (surrogate evidence of community transmission)

■ It is most humbly submitted that the data thus collected pertained only to what was essentially required for protecting the person and the persons in their immediate contact and public from the attack of COVID19 pandemic. The data is of no long-term applicability. The utility of the data is primarily to monitor the health condition of the person under home quarantine during the quarantined period. As pointed out, the daily reports primarily seek to gather the information regarding symptoms developed by the person in home isolation. Once the isolation period is over, the history of how the symptoms had evolved during the isolation period is not at all relevant. There is no need to use the data thus collected any further. It is submitted that the quarantine period is something like an observation ward in a hospital, where there will

be a hospital system which monitors either through physical observation or through a set of devices, the condition of a patient under observation. In the quarantine period prescribed for COVID, all that is required to be assessed is when the patient who is asymptomatic develops any of the symptoms. This can be done by keeping the person in a quarantined place and recording the particulars of the daily symptoms through a form. When large numbers of people are to be monitored simultaneously in a similar manner and any trend in symptoms developing is to be noticed, including perhaps the age group, the geographic location etc, determined health related inferences and further actions can be initiated. The purpose of the data collection is only to facilitate such analysis and trigger action. So there is no need to retain the data for a very long period, not definitely much beyond the quarantine period. The system has the capability to have the data purged/ destroyed at a specified time interval that can be prescribed. Even the queries regarding their co-morbidities gathered only generic names of the disease and not even the degree of its severity was asked. It is also submitted that this information had a direct correlation to possible sources of infection and spread of the virus, as well as vulnerability to the infection. Hence, the data collected was relevant and necessary and does not pose any threat to the privacy or security of the individual. The first respondent has however taken note of the inherent privacy rights and limited its actions to reasonable and necessary requirements.

**■** 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. The further allegation to the effect that details of rations cards and adhaar cards are also being entrusted to the third respondent, is baseless.

37. 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 and that such subjective decisions are left to the Government, which has to act in the best interests of the public more so when such actions do not violate any constitutional mandates and are well within legitimate state aims and proportionate.. Collating this data collected and comparing it with other

available data and giving necessary pointers to the local government required 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.

38.Of the 14 districts and around 1200 local bodies, only less than 100 Grama 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.

39.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).

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

40. The Petitioner does not take issue with the collection of data by the Government per se. However, he has raised concerns about alleged sharing of this data, which purportedly 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**

41. As regards hosting the data being collected through the platform/ software to the [citizencentre.sprinklr.com](http://citizencentre.sprinklr.com), it is submitted that after initial testing, this was changed to [citizencentre.Kerala.gov.in](http://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](http://citizencentre.sprinklr.com). As soon as the url [citizencentre.kerala.gov.in](http://citizencentre.kerala.gov.in) became functional, this has been migrated to therein. 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. The entire data and application is now hosted in the Amazon Cloud Server instance owned by C-DIT and consequently the first respondent.

42. 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.
43. 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/ has been 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 that the data collected above is being processed only in the C-DIT instance using the third party application hosted therein. It is submitted that the Government has now full and exclusive ownership of the data and for analysis of the data, the software of the third respondent, now available with the C-DIT, will be used. Hence, there is no transfer of data to third parties.
44. A large data analytic company like the third respondent, which deals with structured and unstructured data, was engaged primarily to ensure support under two scenarios a) a large inflow of people from other parts of India and abroad once lockdown is relaxed, which has now become a reality; b) in case of a sudden spurt in disease incidence which needs to be carefully managed, which spurt is also increasing after the beginning of the return of expatriates to the State. 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 engaged. The work initially undertaken in an experimental manner to ensure the readiness of the platform for such eventuality. However, the present dedicated instance of the software of the third respondent created within the AWS account of C-DIT fully augments the readiness of the Government to face the situation. It will not have been feasible for a Government agency to develop such scalable platforms and solutions in such short periods of time, as they are not specialists in this field. Subsequent enquiries that the Government had with the National Informatics Centre and the Ministry of Electronics and Information Technology, Government of India, for information system application available with them, suitable for the functional requirements of Kerala, has also met with silence, so far.

45. 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. With the large inflow of people 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 and safeguards will be implemented.

#### **DATA SECURITY**

46. 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 and there is no basis for apprehensions on the use or abuse of data, as the very policies of the third Respondent restrain the same. 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.

47. It is submitted that the Purchase Order with the third respondent was signed only after ensuring the various provisions in the Master Services Agreement / Data Processing Addendum (DPA), which becomes binding on the third respondent on data processing work entrusted to it. A Scrutiny of the Master Services Agreement and Data Processing Addendum, which are integral parts of the purchase order show that the security certifications and processes of Sprinklr includes substantive provisions for Data protection and General Data Protection Regulations of the European Union (hereinafter referred to as “the GDPR” for short) compliance. It specifically provides a GDPR compliant Data Processing Addendum (DPA) to all its customers which includes the EU Standard Contractual Clauses. Further it was ensured that the third respondent is also certified under the EU-U.S. Privacy Shield which binds them to absolute transparency with regard to its data processing operations, including all sub-processors, if any used by them. Moreover, it was ensured that the third respondent holds SOC2 Type2 security certification before they were on boarded and purchase order signed. A very notable feature of the agreement/ purchase order is that it ensures that every employee of the third Respondent, is aware of his/her data protection and confidentiality obligations. Every employee participates in mandatory data protection and information security trainings and is formally obliged to data secrecy. Further it was ensured that the third respondent established a data protection steering committee of key functional leaders throughout the company and also the third respondent appointed an experienced Data Protection Officer. This was relevant when the data was being used in the SaaS application of the third respondent, when employees of the third respondent could have had access to the data. However, it is submitted that none of these safeguards are relevant now as the complete application and data is being managed in the Amazon Web Cloud Server instance of C-DIT and no employee of the third respondent has any access to any data. The only support which the third respondent is providing is for any updation of the application based on the functional requirements suggested by the State, if such occasion arises. Even

for the same, it is only limited technical access to install and plug in to the software and there is no access to the data.

48.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.

49.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.”*

50.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.

51.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

52.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.

53.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.

54.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

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

### **A. Data protection during Transit:**

56. The Secure Socket Layer (SSL)/ Transport Layer Security (TLS) is used, which is the industry standard

### **B. Data protection during Storage:**

57. Ministry of Electronics and Information Technology (MEITY), 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 MEITY, 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 MEITY empanelled Cloud Providers, as they are already MEITY and STQC audited.

58. 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.”

59. Amazon Web Service (AWS) announced that Amazon Internet Services Private Limited (AISPL), an Indian subsidiary of the Amazon Group, which undertakes the resale and marketing of AWS Cloud services in India, has achieved full Cloud Service Provider (CSP) empanelment, and successfully completed the STQC audit from the Indian Ministry of Electronics and Information Technology (MEITY) for cloud services delivered from the AWS Asia Pacific (Mumbai) Region. With this certification, AISPL joins a list of approved providers that meet pre-defined Government standards of quality, availability, and security. With 52 global security certifications, attestations, assurance programs, and quality audits already achieved, such as ISO 9001, SOC1, SOC2, SOC3, and more, AWS is the first global cloud service provider to earn this status in India. The empanelment process includes compliance with new global security standards and guidelines ISO 27017 and ISO 27018. AWS's flexible and highly secure pay-as-you-go cloud services thus, provides adequate and safe infrastructure for the present programme.

#### **C. Data Protection during processing**

60. 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. In the present instance, the application required for processing 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.

61. Data Center and the citizen center App is fully owned and controlled by CDIT. Data encryption is enabled and Firewalls rules are in place which ensure no data can leave the servers. Access requires SSH (Secure Shell) into Access server with 2-FA (Factor Authentication). Alerts are set up for

unusual activity such as brute force where the user account gets locked after 3 consecutive invalid entries and user to root. Alert is sent to the NoC team Data Center and the citizen center App. A full snapshot of the production environment database is performed on a daily basis. Automated Database backups are performed by CDIT. These Backups are stored encrypted.

62.A Log Analysis Audit was conducted to examine and identify any kind of data breach or as to whether any unauthorised access happened with regard to the data and the Software as a Service, now in issue in the writ petition, stored in the Amazon Web Cloud Service licensed to C-DIT The Log Analysis Data for the period from 03/04/2020 to 19/04/2020 revealed that there was no such unauthorised access and data or leakage. From 20/04/2020, as set out herein, the data has been within the sole control and access of first Respondent Government. A true photocopy of Government Order whereby TShe Kerala State Information Technology Mission was authorised by the Government of Kerala to get the log audit done by an empanelled agency, GO(MS) No. 49/2020/ ITD dated 21/04/2020 is produced herewith as **Exhibit – R1 (c)**. The work order dated 22/04/2020 is produced herewith as **Exhibit – R1 (d)**. A true photocopy of the Log Analysis Report dated 23/04/2020 is produced herewith and marked as **Exhibit – R1 (e)**.It is most humbly submitted that an Audit from 27/03/2020, the date of data porting to Amazon Web Cloud Service, can be conducted by STQC under the auspices of the Ministry of Electronic and Information Technology.

63.In so far as the data collected is stored in the Amazon Web Server (AWS) account owned fully by CDIT, which is a Government Institution, thereby ensuring the security of such data; in so far as the Amazon Cloud Web Server, which has signed a Non Disclosure Agreement with the Government of India, is one among the 12 cloud providers empanelled by the MEITY, Government of India and subjected to audit by STQC; in so far as the data is residing in C-DIT control and with it being processed in the servers in the control of C-DIT through the use of the third respondent's software deployed in the control of C-DIT, there is no transfer of data to third party . Further, the first respondent has affirmed that the data will be anonymised prior to transfer, if at all required, and the above clarification affirms that such

transfer will not take place. Therefore, the apprehension of any adverse affect on the national security of our country is unfounded and unwarranted.

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

64. 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 software 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.
65. 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.
66. 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 the person 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).

67. 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).

68. 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 Non Communicable Disease (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.

69. 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 Non Communicable Disease patients, put together will constitute approximately 50 Lakhs persons who need to be under monitoring. The Non Resident Keralites returning to the State and going under surveillance would add further. 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. The system presently is customised with an user friendly interface to capture 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.

70. 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 back to normal operations, 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. The relaxation of interstate travel norms and the return of expatriates to Kerala through Vande Bharat Flight Service has already put the State to a situation of forewarning. Thus, it would be wrong and premature to judge that the issues have tided over and the incidences 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.

71. 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 quite 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 reported daily.

72.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.

73.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. This is absolutely in concurrence with the principle "to err on the side of caution", which is a basic tenet of disaster management.

74.It is further submitted that all these actions were undertaken in a scenario when more than one learned institutions had indicated through scientific prediction models that the State would have to face severity of the pandemic by middle of the year and the health care system, local governance and all related logistics may get trampled with the heavy burden of the pandemic outbreak. At that time the first segment of the lock down was in force, which was enforced from 24<sup>th</sup> March to 14<sup>th</sup> April 2020, but had no indication on what regulations would be brought in after the lifting of the lockdown. It was so expected that the Keralites abroad and in other States would start returning soon on lifting the lockdown and the surge of positive COVID cases would start by the end of April. Hence, at that time it was a pressing requirement to reinforce the preparedness of the State, even to face the most pessimistic

situation and to do everything to protect the citizens. It was in that backdrop all the actions under scrutiny today had taken place. The extension of lockdown thereafter had changed the above situation by providing more time for increasing the institutional systems, as well as allowing organized inflow of Diaspora. In case the extended lockdown was not there, the spurt of pandemic and associated burden on the government system would have been a reality by now. Therefore, if we look upon the actions undertaken from the situations at present only (without considering the averted crisis that was looming over the state by end of March 2020) the need and pressure that was on the government machinery may not be visible enough. Hence, the wisdom of hindsight should not be used to judge the assessment made and actions taken, when the extended lockdown scenario and consequent buying of time for preparation was not in the air.

75. 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. 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.

**WHETHER THE INFORMATION TECHNOLOGY (IT) DEPARTMENT OF THE STATE IS EQUIPPED TO CARRY OUT THE FUNCTIONS THAT IS BEING CARRIED OUT THROUGH THE THIRD RESPONDENT?**

76. 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.

77. 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.
78. 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.
79. 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.
80. 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.

#### **AS REGARDS THE JURISDICTION OF NEW YORK COURTS**

81. 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.

82. Firstly, the choice of jurisdiction i.e., of New York Courts, is a standard form contract of the third Respondent which does not form part of the Privacy Policy. The first Respondent took due care to ensure both legal and technical security of the data being collected and processed, at no cost to the Government. The said data resides in India on cloud services duly approved by the second Respondent within the custody of the Government. Even the software application is within the Government's custody and implemented in the CDIT servers. This was also a well negotiated process considering the value attached to such software. Any data breach or even apprehension thereof therefore pertains to occurrences in India. The Agreement containing the mandate for New York jurisdiction is solely binding on the parties thereto, that is the first and the third respondents. 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 the low risk of any possible dispute 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.

83. 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, if there are any breaches by the said 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 and / or the Central Government to initiate action in India, as a restriction on jurisdiction for civil action does not limit Criminal or regulatory prosecutions or jurisdictions there for.

84. It is pertinent that data resides in India, the software program for processing resides in India and hence there would be no issues of risk to data or security thereof or on and hence there would no issues of jurisdiction. Even if any breach occurs from outside India, Section 75 of the IT Act empowers

initiation of prosecution within India provided such breach impacts a computer or computer resource within India.

85. 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.

86. 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. Any additional civil claims on data breach and agreement violation can be addressed through the courts of New York State as well.

87. 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.”

88. 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.

**As regards averments with regard to the various other clauses of the Master Service Agreement and the date of signing of Purchase Order and the Non Disclosure Agreement**

89. Clause 3 of the Master Service Agreement (MSA) states the term and termination of the agreement – the term is defined as from the effective date of commencement to date of expiration and, in between, either party could terminate the same if any breach pointed out is not cured in 30 days. It states the steps for settling payments and transferring the data in full to the customer on expiration of the term. This amounts to essential and normal conditions of the service procurement, which cannot be viewed as against the interest of the State. Clause 4 of the MSA is on the Fees and Payment, which is actually irrelevant for the present case as the service is availed as a pro-bono service and hence, no payment is involved. The statement that this clause could lead to corruption and financial loss to the public exchequer is wrong as no financial transaction is involved at all. Clause 6 of the MSA is a standard indemnification, which defines the liabilities of each of the parties and that no way violates the interest of the state. Clause 7 of the MSA describes the Limitations of Liability, that are the cases in which the parties would not be held responsible, and none of that is in conflict with any of the provisions of IT Act. Clause 8 of the MSA clearly spells out that the customer or the company would not use any confidential information of the other party for any purpose other than necessary to perform its obligatory task and also clearly states that neither of the party will disclose any

confidential information to any third party without prior written consent of the disclosing party. This actually protects the confidentiality of the data and ensures data security and cannot be stated to be highly unethical and in violation of Article 21 of the Constitution.

90. The purchase order document with all its annexure were made available by the Company on 24<sup>th</sup> March 2020 itself. Affixing signature on the Purchase Order was done by the IT Secretary formally on 2<sup>nd</sup> April 2020 after trial data collection and further clarifications of details and obtaining a technical scrutiny by the IT Support team. The signing was not done on blank paper as alleged. The document was first signed by the Principal Secretary, E&IT and its scanned copy was mailed to the company, which was returned by them by mail itself after affixing the signature from their side. This was a normal procedure and valid as both parties honour the signatures.

91. The purchase order and the enclosed documents were appropriately signed by both parties (IT Department and M/s Sprinklr Inc) on the mutually honoured consensus that the license for use of the SaaS platform would be made available from 25<sup>th</sup> March 2020 and would be available for State of Kerala till 24<sup>th</sup> September 2020. The software platform was accordingly, made available from 25th March 2020 itself. Both parties involved, upholds the period of validity and do not have any dispute on the dates. Hence, the Purchase Order being signed on a later date, due to the delay in functional formalities, does not results in any diminution of the value or authenticity of the document. The mode of execution of the said Order Form was also undertaken expeditiously to avail of the application at the earliest, given the urgency and seriousness of the situation. The validity of an Order Form being concluded through the means as set out above are also valid and sustainable in law.

92. The Mutual Non-Disclosure Agreement was one of the appended documents of the purchase order and was part and parcel of the said purchase order. So, the same also have validity from 25<sup>th</sup> March 2020 itself. The decision for affixing signature of the NDA formally, was taken on 14<sup>th</sup> April 2020, only as an additional measure for mitigating any apprehension on the security of the application.

**AS REGARDS THE ALLEGATION THAT THE OTHER DEPARTMENTS  
WERE SURPASSED BY THE SECRETARY OF THE IT DEPARTMENT  
OF THE STATE AND THAT THE NOD OF THE LAW DEPARTMENT  
WAS NOT OBTAINED**

93. 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. There is no ground or basis for apprehensions of misuse after the term of engagement, as the data is in the control of the Government and in any event, the very provisions of the Agreements with third Respondent restrict and limit data to usage for the purpose it was collected for. 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 , but did not require any consideration with the said Department at all.

94. The decision for the procurement of the SaaS application, deployed and developed by Sprinklr, the third respondent, was not a single-handed decision of the Principal Secretary of the Electronics and Information Technology Department (hereinafter referred to as the “E & IT Department” for short). The decision was taken based on clear consultations and scrutiny within the E&IT Department of the State in a committee –the IT Support Team- comprising of the heads of all institutions under the Department as well as representatives of Health Department and Local Self Government Department and State Disaster Management Authority (SDMA). The IT Department and State Disaster Management Authority (SDMA). The IT Support Team was formed within the Department to take forward the necessary interventions with regard to supporting COVID 19 control activities during lockdown period when the Department Sections were not in the fully functional mode. Secretaries of the Departments such as Health and Local Self Government and SDMA also attended some of the meetings and outlined their field level requirements and identified suitable officers from

the respective departments for attending the regular meetings of the IT Support Team for working out the requirements in greater granularity. The team had made detailed scrutiny of the documents and technical aspects of the SaaS application and submitted the recommendations in affirmative to the Principal Secretary, E&IT Department for taking forward the matter. Hence, the actions taken by the Principal Secretary, E&IT Department to sign the document and avail the SaaS application had sufficient scrutiny and consensus on technical and functional requirements being met.

**AS REGARDS THE ALLEGATION THAT THERE HAPPENED TO BE VIOLATION OF THE PROVISIONS OF ARTICLES 298, 299 AND 300 OF THE CONSTITUTION OF INDIA**

95. The transaction between E&IT Department and the Sprinklr inc is limited to the procurement and use of a Software as a Service (SaaS) application developed and deployed by M/s.Sprinklr Inc. It was procured as free of cost service for six months for Kerala to manage the data analysis requirement that could arise in case of a surge in COVID19 spread. The paper work undertaken for the same was issue of a Purchase Order with a set of appended standard terms and conditions, that usually associates with any SaaS tool. There was neither any drafting or executing of agreement involved nor any financial transaction done. Issue of a formal purchase order pertaining to a pro-bono service procurement is within the authority and responsibility of the administrative head of the department. Therefore, the contention that the action taken in this regard is bound by Articles 298, 299 and 300 of the Constitution (which pertains to drafting and execution of contracts) does not have any standing. In any event the Government is seized of this and it is imperative in the interests of justice that the Government of Kerala be allowed to complete its review and decision in this regard.

**AS REGARDS THE CONTENTIONS WITH REGARD TO GO (MS)**

**No. 79/2020/ GAD dated 20/04/2020**

96. The Government, as per GO (MS) No. 79/2020/ GAD dated 20/04/2020, appointed a two member Committee to look into the relevant aspects with regard to the arrangements made with the third respondent for extension of their software as a service and to submit a report regarding the same. A true photocopy of GO (MS) No. 79/2020/ GAD dated 20/04/2020is produced

herewith as Exhibit R1(f). The Committee was constituted to appraise the Government of the activities carried out in this regard and to suggest the future course of action. The Committee was constituted for the reason that the Government was committed not to create panic among the citizen or to ignore the apprehensions raised especially in the situation where a pandemic is looming over the country.

**AS REGARDS THE ALLEGATIONS REGARDING THE ENGAGEMENT OF SPRINKLR AMOUNTING TO OFFENCES UNDER THE PENAL CODE AND THE PC ACT**

97. It is alleged that in the event of data breach, offences under Sections 463 to 471 of the Penal Code will be attracted. This allegation is patently misconceived and unsustainable. These provisions of Indian Penal Code, 1860 ("IPC") apply to forgery. There is no offence of forgery, making of false document or using as genuine any forged document. In the said circumstances, the said allegation is unsustainable in law. There has been no case brought out regarding the receipt of gratification or illegal remuneration or obtaining any valuable thing for the purpose of engaging Sprinklr. In the said circumstances, no offence under Sections 7 to 11 of the PC Act will be attracted. It is most humbly submitted that the allegations regarding commission of offences are solely based on speculations, surmises and conjectures and not based on any cogent material, much less any material and the same are clearly vexatious and malicious baseless allegations raised with vested interest.

**POINTS OF LAW TO BE URGED**

98. The issue of maintainability of the Writ Petitions ought to be addressed first, as a preliminary issue, as the Petitions filed are not maintainable or sustainable and the same ought to be rejected at the outset, as they are based on apprehensions, speculations, conjecture and surmises. Intervention through these Petitions in the just, reasonable and proportionate execution of the functions of the Government of Kerala has and will continue to cause grave and irreparable harm and damage. It is imperative that the resources, time and energy of the Government be best utilised to combat the unprecedented threat of COVID19 and not be diluted or diverted for countering such baseless and vexatious proceedings.

99. 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.

100. 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 necessary, expedient and warranted 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.

101. According to Section 2 of the Epidemic Diseases Act, 1897, State Government has the powers to inspect persons suspected of having contracted the disease as a measure to prevent the spread of the disease. Inspecting and gathering the health status of persons under home quarantine is well within these premises and cannot be viewed as a violation to their privacy. It is a precautionary measure to protect the citizens from the pandemic.

102. As per Section 4 (2) (b) of the Kerala Epidemic Diseases Ordinance, 2020 (Ordinance No. 18 of 2020), the Government has the power 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 epidemic disease and as per clause (d) thereto, the Government can also take such other measures as may be necessary for the regulation and prevention of epidemic diseases as decided by the Government. On this count also, the collection of information by the Government, for the purpose of management of the COVID pandemic, has the sanction of law.

103. 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.

104. 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 own 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.

105. 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.

106. 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)"*