6 –ാം സമ്മേളനം

സ്പ്രിംഗ്ലർ കരാർ അന്വേഷണം

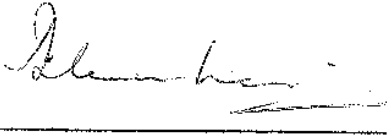| ചോദ്യം	ഉത്തരം
ശ്രീ പി സി വിഷ്ണുനാഥ്	ശ്രീ. പിണറായി വിജയൻ (മുഖ്യമന്ത്രി)
(എ) സ്പ്രിംഗ്ലർ കരാർ സംബന്ധിച്ച് അന്വേഷണം നടത്തിയ മാധവൻ നമ്പ്യാർ കമ്മിറ്റി റിപ്പോർട്ടിന്റെ പകർപ്പ് ലഭ്യമാക്കുമോ;	(എ) മാധവൻ നമ്പ്യാർ കമ്മിറ്റി സമർപ്പിച്ച റിപ്പോർട്ട് അനുബന്ധം-1 ആയി ചേർക്കുന്നു.
(ബി) സ്പ്രിംഗ്ലർ കരാർ സംബന്ധിച്ച് തുടർന്ന് അന്വേഷണം നടത്തിയ കെ.ശശിധരൻ നായർ അദ്ധ്യക്ഷനായ കമ്മിറ്റിയുടെ റിപ്പോർട്ടിന്റെ പകർപ്പ് ലഭ്യമാക്കുമോ?	(ബി) കെ.ശശിധരൻ നായർ കമ്മിറ്റി സമർപ്പിച്ച റിപ്പോർട്ട് അനുബന്ധം-2 ആയി ചേർക്കുന്നു.

സെക്ഷൻ ഓഫീസർ

Sprinklr Usage by Government of Kerala

COMMITTEE REPORT

ACKNOWLEDGEMENT

We wish to thank the Government of Kerala for all the support rendered, to enable us to conduct the enquiry. Our special thanks to Shri Mohammed Y Safirulla, Secretary Information Technology, Government of Kerala for his proactive and prompt response, despite constraints.

Shri M. Madhavan Nambiar

Chairman

Dr. Gulshan Rai

Member

4713861/2020/GAD(AIS-A)

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Kerala was the first State in India to report COVID-19 cases in January 2020, significantly earlier than when a nation-wide lock down was effected on 23rd March 2020. As a progressive state, Kerala, has successfully in the past battled pandemic like situations especially related to the Nipah Virus in 2018-19.

The Kerala Disaster Management Authority (KSDMA) had projected in its studies that the state would be burdened with far more COVID-19 cases than the existing healthcare facilities could accommodate. Independent studies projected more than 9 million cases by the end of April in the state. It was felt that the state needed to quickly upgrade its monitoring facilities related to contact tracing and working on obsolete Excel spreadsheets would not help it with the expected deluge of COVID-19 cases.

The IT Department entered into multiple agreements with US-based Sprinklr Inc. as it was felt that the state needed multi-dimensional data-analytics solutions related to COVID-19 cases. US-based Sprinklr Inc., which has a CEO who is of Kerala origin, had offered its Software as a Service (SAAS) products for the purpose of COVID-19 containment on a pro-bono basis and the offer was to host their data analytic platform in India, process the data and provide analysis quickly.

It was decided that data will be initially hosted in the computers of Sprinklr Inc. hired by them at Amazon Web Services (AWS) Mumbai. The entire data and applications would then be transferred to computers of CDIT as soon as the same was ready. The data was however, to be managed by Sprinklr Inc. at all times. This process continued till the early part of the first week of April 2020. Data from the computer systems of Sprinklr Inc. was transferred to computer systems of CDIT on the 17th of April 2020.

Certain issues related to data privacy and security were raised in the public domain as well as the process of engagement of Sprinklr Inc and the government constituted a committee on 20th April 2020 by the **GO (Ms) No. 79/2020/GAD** consisting of Chairman, Shri M Madhavan Nambiar, IAS (Retd.), and Dr Gulshan Rai, former Cyber Security Coordinator, Government of India in place by **GO (Ms) No. 146/2020/GAD** dated 13th Aug 2020.

The Committee followed a detailed methodology involving virtual interactions and questionnaires to the stakeholders involved and also studied in detail the Agreements which were executed by Mr M. Sivasankar IAS, Principal Secretary, Department of Information Technology, Government of Kerala with Sprinklr Inc.

On analysis, prima facie, it was clear that all the Agreements were not negotiated or discussed threadbare and it granted omnibus rights on customer content to Sprinklr Inc. It would be very difficult to enforce penalty for any violation of the Agreement Clauses (including Breach of Privacy, Confidentiality and Security of Data) as the Jurisdiction of the Agreements was at Courts of New York, USA.

It is clear to the Committee, that the Principal Secretary, Information Technology Department, did not comply with laid out procedures, in executing the Agreement with Sprinklr Inc, acted unilaterally, without any discussions with other stakeholder arms of the State Government including the Health Department, the Law Department and did not even inform the Chief Secretary of the Government of Kerala.

By-passing the Crisis Management Group, headed by the Chief Secretary, the then Principal Secretary Information Technology installed a Digital Platform for managing the data complexities arising out of the COVID-19 pandemic. The Agreement with Sprinklr Inc. was also executed in a hasty manner without any approval from the Chief Minister, who also holds the Information Technology portfolio.

The Committee has also found certain lacunae in the capabilities of the Information Technology Department in its understanding and selection and implementation of data analytic digital platforms. The gaps and weaknesses are related to technical skills and lack of processes. The Committee had recommended several measures to bridge the gap and weakness of the system particularly the upgradation of the skills, processes and implementation of digital platforms. These recommendations include; putting in place robust measures for enhancing the quality of IT infrastructure, with a specific focus on cyber security and data protection of citizens; strengthening governance structures to ensure a clear system of checks and balances and strong mechanisms for convergence and coordination across departments.

2. BACKGROUND

Kerala was the first State in India to report the incidence of COVID-19 virus way back in January 2020. Leveraging the strength of its decentralized healthcare infrastructure and experience gained from effective containment of the Nipah outbreak in 2018 and 2019, the Government of Kerala had deployed effective strategies to contain the spread of COVID-19, in January itself. However, the return of Keralites from other parts of the globe where the pandemic had devastating effects had once again increased the incidence of the disease during the month of March. The Kerala Disaster Management Authority (KSDMA), through its various studies had predicted exponential growth in the number of patients with people requiring critical hospital care estimated to be far more than the capacity of the state's organized health care facilities. KSDMA predictions in this regard are given in the table below. These projections, which were quite alarming, were made on 28th March 2020.

Expected COVID-19 incidence in Kerala by April third week	1.25 Cr
Symptomatic patients by April third week	90 Lakhs
People needing hospitalization by April third week	9 Lakhs
People who would require ICU treatment by April third week	2 Lakhs

(SOURCE: KSDMA Report)

Similarly, a group of experts associated with the Centre of Disease Dynamics, Economics & Policy, and Johns Hopkins University estimated that by 25th of April, there would be 80 Lakh people in Kerala affected by COVID-19. It was also seen that in several parts of the world, like Italy, USA, Spain etc. the existing healthcare system became extremely stressed resulting in substantial casualties.

Kerala, with its high population density and influx of a large number of people from infected regions was extremely susceptible to widespread virus outbreak and casualties in the short run. Kerala also had a large vulnerable population of about 50 lakhs - those who had comorbidities and who were above 60 years of age.

Kerala's strategy for containing the disease was to quickly track & trace, isolate alongside regular symptoms monitoring. The potential contact data of people who could be infected was gleaned from flight passenger manifests, spreadsheets from various points like airports,

hospitals, railway stations, supermarkets, WhatsApp messages from various points. As the number of patients & their potential contacts reached a very high number, manual tabulation of such disparate information in unsecure forms like spreadsheets became very cumbersome & Kerala realized that this method could not be scaled effectively.

3. FACTS OF THE CASE

Considering the need for a multi-dimensional data-analytics solution, an informal Technical Group chaired by the Principal Secretary, IT Department of Government of Kerala was set up. It comprised of Heads of all institutions under IT Department, viz., Director KSITM and CDIT, Director IIITM-K, CEO IT parks and MD KSITIL. Representatives of other concerned Departments such as health, LSGD and KSDMA also attended the meetings. Mostly the meetings were conducted through virtual mode - WhatsApp. Nevertheless, few meetings did take place in the physical presence of the members. The IT Department had identified Sprinklr Inc. – a Company offering Software as a Service (SAAS) and specializing in multi-dimensional data analysis of structured & unstructured data. The said company had earlier got in touch with the government and offered its product for the purpose of COVID - 19 containment on a pro-bono basis. The offer was to host their data analytic platform in India, process the data and provide analysis quickly.

In the Committee's inquiry with the then Secretary-IT, Mr. M Sivasankar IAS, and the other Officers of IT Department, it was informed that Sprinklr Inc. was chosen & implemented as a one stop solution for all data needs for managing COVID-19 pandemic due to the following reasons:

> ➢ The technical group of the IT Department did an evaluation of the product and it was found that the product would serve the purpose.
> ➢ The product was offered free of cost.
> ➢ Ease of deployment.

It was decided that data will be initially hosted in the computers of Sprinklr Inc. hired by them at Amazon Web Services (AWS) Mumbai. The entire data and applications will be transferred to computers of CDIT as soon as the same was ready. The data was however, to

be managed by Sprinklr Inc... The appropriate form for collection of data in the field was designed by the concerned Department of the Kerala Government with the assistance of CDIT.

Sprinklr Inc. had set up their Data Analytic Platform on the computer systems hired by them on the cloud system of Amazon Web Services (AWS) at Mumbai. The data was collected by the field staff of the Kerala government and transferred directly to the computer systems of Sprinklr Inc. The record of 1.82 lakh people were entered into the Sprinklr Inc. This process continued till the early part of the first week of April 2020. Data from the computer systems of Sprinklr Inc. was transferred to computer systems of CDIT on the 17th of April 2020.

The timelines of main events are summarized in chronological order in the table below:

Sl No:	Event	Date
1	Data start uploading in the Cloud computing facility hired by Sprinklr Inc. at Amazon Web Services, Mumbai.	25th March 2020
2	Signing of NDA & Agreement with Sprinklr Inc. effective 25th March 2020	2nd April 2020
3	Duration of the Agreement	6 months w.e.f. 25th March 2020 i.e. upto 24th September 2020
4	Clarification on data rights & confidentiality obligations in connections with Sprinklr Inc.	12th April 2020
5	Date of transfer of Database from Sprinklr Inc. AWS account to CDIT AWS account (Hon'ble Chief Minister, on 15th April 2020, announced the transfer of Data from Sprinklr Inc. to CDIT)	17th April 2020
6	Uploading of data in Computer servers of CDIT at AWS, Mumbai	20th April 2020
7	SAAS application transfer from Sprinklr Inc. AWS to AWS account of C-DIT	22nd April 2020
8	Instruction from Govt to Sprinklr Inc. to delete the stored data from its servers as the data has been migrated to CDIT's AWS servers	16th May 2020
9	Confirmation on permanent deletion of data by Sprinklr Inc.	21st May 2020

4713861/2020/GAD(AIS-A)

10	Cancellation of the Agreement on expiry of time period contract	24th September 2020

4. CONSTITUTION OF THE COMMITTEE

Even though Sprinklr Inc., a company owned by an entrepreneur of Kerala origin had given its services Pro Bono for the Government of Kerala for COVID-19 management, certain issues were raised in the public domain regarding the privacy and security of the data as well as the process of engagement of the company. Hence, the government constituted a committee on 20th April by the **GO (Ms) No.79/2020/GAD** consisting of Shri M Madhavan Nambiar, IAS (Retd.), former Civil Aviation Secretary & former Special Secretary, Information Technology, Government of India as Chairman and Shri Rajeev Sadanandan IAS (Retd.), former Additional Chief Secretary (Health & Family Welfare Department, Government of Kerala as member, to get the above issues and other relevant aspects examined.

Subsequently, as Shri Rajeev Sadanandan was entrusted with the duty of advising the Hon. Chief Minister on matters related to COVID-19 epidemic; based on the suggestion of the Chairman, Government nominated Dr Gulshan Rai, former Cyber Security Coordinator, Government of India in place of Shri Rajeev Sadanandan by **GO (Ms) No. 146/2020/GAD** dated 13th August 2020.

1	Committee formation by Government of Kerala	20th April 2020
2	Nomination of Shri Gulshan Rai instead of Shri Rajeev Sadanandan in the committee	13th August 2020

5. TERMS OF REFERENCE OF THE COMMITTEE

As per the GO (Ms) No.79/2020/GAD, the Committee was to examine the following issues related to Sprinklr Inc.

4713861/2020/GAD(AIS-A)

1. Whether the privacy of personal and sensitive data of individuals has been protected under the Agreements entered into with Sprinklr Inc.

2. Whether adequate procedures have been followed while finalizing the arrangement with Sprinklr Inc.?

3. Whether deviations, if any, are fair, justified and reasonable considering the extraordinary and critical situation the State was facing at the relevant period?

4. Any other suggestions for future guidance.

6. PETITION IN THE HON'BLE HIGH COURT OF KERALA

In the meantime, a bunch of writ petitions were filed in the Hon'ble High Court of Kerala in April 2020 on the issues relating to privacy and security of health data as well as on Agreement and contract awarded by the Kerala Government. to Sprinklr Inc. Kerala Government, Union of India and Sprinklr Inc. apart from other Departments of Kerala Government are respondents. Some more writ petitions were filed on 24th June 2020. The Kerala Government filed their affidavit in all the writ petitions in the Hon'ble High Court of Kerala on 22nd April 2020. Kerala Government mentioned in the court about setting up of the Committee as mentioned in para 3. The petitions came up for hearing for admission on 24th April 2020 on which day, an interim order was passed by the Hon'ble High Court. The operative part of the order is captured below:

"22. Therefore, as at present, we deem it apposite to confine our focus on ensuring that there is no breach of confidentiality of the data collected by the State and processed by Sprinklr Inc., and since we are not in a position to conclusively persuade ourselves that the terms of the impugned contract would effectively ensure it, we feel it requisite to issue the following directions as an interim measure; also so as to enable this Court to obtain an overall control over the conduct of the parties in terms of the contract with respect to data confidentiality.

23. We are also guided to do so, impelled by the singular intent to ensure that there is no "data epidemic" after the COVID-19 epidemic is controlled.

4713861 2020/GAD(AIS-A)

24. Resultantly:

(a) We hereby direct the Government of Kerala and its concerned Departments to anonymise all the data that have been collected and collated from the citizens of the State with respect to the COVID-19 epidemic, as also with respect to all data to be collected in the future and to allow Sprinklr Inc. to have further access to any such data only after the process of anonymisation is completed.

(b). The Government of Kerala is directed to inform every citizen, from whom data is to be taken in future, that such data is likely to be accessed by Sprinklr Inc. or other third party service providers and their specific consent to such effect shall be obtained in the necessary forms or formats.

(c). We hereby injunct Sprinklr Inc. from committing any act which will be, directly or indirectly, in breach of confidentiality of the data entrusted to them for analysis/processing by the Government of Kerala under the impugned contract/s; and that they shall not disclose or part with any such data to any third party/person/entity – of whatever nature or composition – anywhere in the world.

(d). We further order that Sprinklr Inc. shall not, directly or indirectly, deal with the data or any part of it entrusted to them by the Government of Kerala under the impugned contract/s, in conflict with the various confidentiality clauses/caveats therein; and that they will forthwith entrust back all such data to the Government of Kerala as soon as their contractual obligation, as regards its analysis/processing, is completed as per the requirements under the impugned contract/s.

(e). Since the Government of Kerala has taken the position before us that, according to them, no data is available with Sprinklr Inc. as of now, any residual or secondary data available with the latter shall be immediately entrusted back by them to the Government and this shall be treated as a peremptory order.

(f). As a necessary corollary to the above directions, we further injunct Sprinklr Inc. from advertising or representing or holding over to any third party/person/entity – of whatever nature or composition – that they are in possession or have access to any data regarding COVID-19 patients or persons vulnerable/susceptible to it; and that

4713861/2020/GAD(AIS-A)

they shall not use or exploit any such data, or the name and the official logo of the Government of Kerala, directly or indirectly, for any commercial benefit and will deal with such in full confidence to the citizens of Kerala.

List these matters on 18.5.2020 for further consideration, within which be discussed in the appropriate paras of this report."

7. METHODOLOGY AND QUESTIONNAIRES

The committee followed a structured evidence-based approach in undertaking its work. All the meetings were held virtually. A Three-Tiered approach was followed. The 1st-Tier consisted of initial briefing on the case by the IT Department of the Kerala Government. The information, documentation and facts of the case were sought on emails. The information and documents so received were analysed. The 2nd-Tier comprised of the preparation of detailed questionnaires and sending to such key officials of the Technical Committee set up by IT Department, for providing necessary additional information on their specific roles and measures which were adopted in the selection of Data Analytic Platform, selection of Sprinklr Inc, decision making process, collection of data, implementation and mechanism of ensuring security and privacy of Data. The questionnaires were sent to four officials and Principal Secretary, IT Department. Verbal interactions were had with the then Chief Secretary, Mr Tom Jose, and the Health Secretary, Dr. Rajan. N. Khobragade Government of Kerala. The responses received from these officials were analysed. The 3rd-Tier detailed interactions were held with all such officials to whom questionnaires were sent. The report of the committee is based on the information provided officially and interactions made with these officials.

8. AGREEMENT WITH SPRINKLR INC.

Mr. M Sivasankar, Principal Secretary (IT), on 2nd April 2020 executed an Agreement with Sprinklr Inc. The Agreement was effective from 24th March 2020. It comprised of two documents, namely: -

1. Sprinklr Contracts FAQ: Who is Sprinklr and What do we Do?
2. Mutual Non-Disclosure Agreement.

4713861/2020/GAD(AIS-A)

Sprinklr Inc. executed another Agreement dated 12th April 2020 with Mr. M. Sivasankar, Principal Secretary (IT) titled "Data Rights and Confidentiality Obligations in Connection with Sprinklr Donation of Software".

These Agreements are limited to hiring and use of SAAS software application developed and deployed by Sprinklr Inc. Sprinklr Inc had made available their services on a Pro Bono basis. The Agreements had clauses regarding obligations to preserve the Confidentiality, Privacy and Security of the data. The Agreements bound the parties not to disclose any information to any third party without prior written consent of the disclosing party. The important clauses relating to Definition of Content, Jurisdiction, Right of Usage of Content and Data Hosting in as provided in these documents are as under: -

1. **"Content"** means Inbound Content, Customer Content and informational content entered into the Sprinklr Account

2. **"Customer Content"** means any material that is (i) entered into the Sprinklr Inc. account by Customer, an Agency or employee on behalf of or under the direction of Customer or

   (ii) Published through the Sprinklr Account to the connected Services for which Sprinklr has Connected Services Authorization.

3. **"Inbound Content"** means any information published on any Connected Service not created by a Customer User. Such information includes but is not limited to, in whatever form and/or nature, text, data, graphics, photos, audio, video, electronic messages, trademarks and other identifiers.

4. **"Miscellaneous"** This Agreement shall be governed by the laws of the State of New York, without reference to conflict of laws principles. Any suit to enforce this Agreement shall be brought exclusively in the Borough of Manhattan, New York, and the parties hereby submit to the personal jurisdiction of such courts and waive any venue objection. This document contains the entire Agreement between the parties with respect to the subject matter hereof. Any failure to enforce any provision of this Agreement shall not constitute a waiver thereof or of any other provision hereof. This Agreement may not be amended, nor any obligation waived, except by a writing

471386/2020/GAD(AIS-A)

executed by both parties. In the event any term of this Agreement is found by any court to be void or otherwise unenforceable, the remainder of this Agreement shall remain valid and enforceable as though such term were absent upon the date of its execution. Neither party may assign this Agreement without the express written consent of the other party, and any prohibited assignment shall be void; provided that either party may assign this Agreement pursuant to a merger, acquisition or sale of all or substantially all of such party's assets except in the event that the proposed assignee is a competitor of the other party. This Agreement shall bind and inure to the benefit of these parties and their successors and permitted. (Part of Mutual Non-Disclosure Agreement)

5. **"Clause related to hosting of data"** All data uploaded by any party and by any means to the Citizen Experience Management Platform by or from Kerala or its citizens is and will be hosted within the geographical boundaries of India and can be 'moved to whatever server or data centre that meets technical requirements and that Kerala specifies, at any time. (Part of Data Rights and Confidentiality Obligations in Connection with Sprinklr Donation of Software)

6. **"2.5** Customer grants to Sprinklr during the term of this Agreement a royalty-free, non-exclusive, non-transferable, worldwide right and license: (i) to copy, cache, store, reproduce, perform, display, use, distribute, transmit and generally make available the Customer Content in electronic form via the Internet, through wireless communications services and social media through the Platform in order to provide the Sprinklr Services to Customer in accordance with this Agreement; and (ii) to access Customer's accounts on the Connected Services in order to provide the Sprinklr Services. (Part of Master Service Agreement)

All the clauses brought in Para 8 hereinabove are important from the point of view of Term of Reference of the Committee.

9. CONTRACT ANALYSIS – CLAUSES REGARDING STORING OF DATA & OMNI RIGHTS TO SPRINKLR

The important clauses relating to Security, Privacy and Confidentiality of Data in the Agreement executed by the Principal Secretary, IT Department with Sprinklr Inc. have been

brought out in Para 8 here in above. The Committee has noted that all the Agreements are in the standard format of Sprinklr Inc. and do not appear to have been discussed and negotiated with reference to the instant case where services were being provided on a Pro Bono basis. The Agreement granted omnibus rights on customer content to Sprinklr Inc. and it will be difficult to enforce the responsibilities and liabilities on Sprinklr Inc. for any violation of the Agreement Clauses (including Breach of Privacy, Confidentiality and Security of Data) as the jurisdiction of the Agreements was at Courts of New York. These clauses are clearly not in the interest of the State of Kerala.

10. SALIENT DETAILS OF THE RESPONSE RECEIVED FROM PARTIES

The Secretary, Department of IT, Kerala Government had provided the background note and information relating to the process which was followed for consideration and the decision to engage Sprinklr for using their Data Analytic Platform. There were, however, no structured records made available which could be examined by the Committee to address issues stated in the terms of reference of the Committee.

There were several disconnected points which needed reliable information and evidence for arriving at definitive conclusions and recommendations. The Committee, based on the information provided in the background note by the IT Department decided to interact with Mr. M Sivasankar the then Principal Secretary, IT Department, the present Secretary, IT Department, Mr. Mohammed Y Safirulla, Director, CDIT; Managing Director, State IT Infrastructure Ltd and Director IIITM-K.

The Committee was apprised that these officials participated in the decision-making process for suggesting implementation of appropriate IT platforms and the selection of a Digital Analytics Platform (SaaS application of Sprinklr Inc.). The Committee interacted with these officials through the video platform. The Committee also interacted with key representatives of Sprinklr Inc. which included the CEO, General Counsel and technology domain experts of Sprinklr Inc.

It emerged from the interaction that an informal discussion group was formed within the IT

471386/2020/GAD(AIS-A)

Department as an "IT Support Team" which met regularly, and discussed implementation plans that could strengthen the state response to the COVID-19 pandemic scenario. The meetings of the IT Support Team were chaired by the Principal Secretary of the IT Department and comprised of Heads of all Institutions under the IT Department and few more experts apart from the above-named officials.

The interaction provided somewhat varied versions of discussions, deliberations and their roles in the IT Support Group. The then Principal Secretary, IT Department, however, stated that the said IT Support Team was in fact part of a larger group which used to meet every day after 5pm and that was steering all aspects of the COVID-19 pandemic in the State. The larger group also included representative of the Health Department. Some of the meetings of the said group were participated by the Member Secretary, Kerala State Disaster Management Authority and Additional Chief Secretary, Revenue and Disaster Management. No structured minutes of meetings were prepared or recorded.

Two of the members namely Director, IIITM-K and MD Kerala State IT Infrastructure Ltd also examined the Techno-Legal aspects of the proposal of Sprinklr Inc. The Director, IIITM-K stated that he was under the impression that log analysis of transactions carried on at the Digital Platform installed by Sprinklr Inc. will be undertaken by CDIT to ensure aspects relating to privacy and security of data processed by the Digital Platform. He, however, in general expressed his ignorance on Legal and Contractual issues of the Agreement as well as subsequent involvement in the project.

The MD, Kerala State IT Infrastructure Ltd, on the other hand, insisted that adequate provisions were built in the Agreements to ensure the privacy and confidentiality of the data stored and processed in the SaaS Platform of Sprinklr Inc. He however could not comment on the process of verifications and mechanisms implemented by Sprinklr Inc. It was the responsibility of CDIT to check and verify implementation of technical and procedural measures to ensure security and confidentiality of citizen data. It clearly emerged that Kerala State IT Infrastructure Ltd was only helping the IT Department as Advisors and the responsibility relating to legal vetting of Agreement and technical implementation was of the IT Department. Mr M. Sivasankar, while strongly defending the utility of the Agreement and overall process adopted in engaging with Sprinklr Inc, however, admitted constraints in

4713851/2020/GAD(AIS-A)

expertise in the area of Cyber Security in general in the State and more so on the digital platforms.

11.MEASURES TO PROTECT THE PRIVACY AND SECURITY OF DATA AND SECURITY AUDIT CONDUCTED BY STQC

The committee was informed that the state government had issued several circulars to all concerned to take appropriate measures to protect the confidentiality, privacy and security of the data during the transit, processing and residing in the systems. It was also stated that Sprinklr Inc. had ensured that the data while residing in their cloud computer systems AWS was encrypted to avoid any stealing of the data.

The Kerala State IT mission had also entrusted the task to conduct the security audit of the data at the AWS server of Sprinklr Inc. to a CERT Empaneled auditor. Subsequently, STQC, an Agency of the Ministry of Electronics and Information Technology (MEITY) was also requested to conduct similar security audit which was earlier undertaken by the Empanelled Auditor. For the purpose of the audit, CDIT had given access of the log file to STQC on 17th July 2020. The access to the Logs was provided via the following link:

"https://awslogsforaudit.s3.ap-south-1.amazonaws.com/log.tar.gz"

The report outlines the following:

1. As per the time stamp mentioned in the STQC report, the Log file was for the period from 3rd April 2020 to 19th April 2020. It is Important to mention that the data collected from the fields Started flowing into AWS servers of Sprinklr Inc. from 25th March, 2020. The data was transferred to the CDIT on 15th April to 17 April 2020.

2. The Log file contained details of applications. Logs of Database, access and other transactions were not made available to STQC. Database Logs were restricted only to those events for which an error or a warning was flagged.

4713861/2020/GAD(AIS-A)

3. The scope of the audit was limited to third-party analysis of the submitted Log file only.

4. STQC had requested for additional information relating to the application, database and network architecture. The same was not provided to STQC.

5. The log reflects that public as well as private IP's access the application.

6. The analysis of log reflects outbound data of the range varying few Megabytes to Gigabytes during the period to some Private IP addresses which belonged to AWS thereby indicating data transfer to some other accounts at AWS. STQC could not correlate the outbound data as the clarifications as well as the database logs and network diagram were not provided. The details of these IP's could have been provided only by either AWS or Sprinklr Inc.

The Committee also noted from the information provided by the IT Department of Kerala that the Joint Secretary of the IT Department, on behalf of the Principal Secretary to the Government of Kerala, had issued a letter dated 16th May 2020 directing Sprinklr Inc. as follows: " I am to inform you that since the entire data has now been transferred to the government owned cloud web space in Amazon Web service, managed and controlled by CDIT, the data if any available in the earlier instance with Sprinklr Inc. shall be destroyed and the same shall be confirmed."

The Sprinklr Inc. wide letter dated 21st May 2020 to the Principal Secretary, IT Department stated: "We are in receipt of your letter dated 16.05.2020, instructing Sprinklr to delete all remaining data, from the period prior to the passing of the Order dated 24.04.2020, by the Hon'ble High Court of Kerala, in the matter cited under reference above.

It is hereby confirmed, that acting under the instructions of the Government of Kerala, Sprinklr has permanently deleted all such data available and remaining on its servers, from the period prior to the aforesaid Order dated 24.04.2020."

Prior to the said letter dated 16th May, a letter was also issued by the IT Department to CDIT and KSITM directing them that the data collected and collated from the citizens of the state in

connection with COVID-19 containment activities should be anonymized before the same is shared with any third-party service provider/software (Sprinklr Inc in the instant case) used for the processing of data. The access of such data should be allowed to any third-party service providers/software as per the Agreement, only after completing and ensuring the process of migration. This was applicable to all the data already collected and to be collected in future with respect to COVID-19 and should be used only for the purpose for which it has been collected.

It may be noted that there is a variation in the understanding and confirmation provided by Sprinklr Inc. with respect to the direction given by the State Government

After studying the security audit report submitted by STQC and other information, the committee is of the view that no conclusion can be drawn regarding the flow of data out of the computer servers of Sprinklr Inc. storing and processing of the data sent by field offices of Kerala Government. The Committee could not get any answer regarding not providing Logs of AWS systems of Sprinklr Inc. w.e.f. 25th March 2020 and why only limited and truncated log files were provided to STQC by CDIT. The Committee did not get any answer w.r.t anonymization of data handed over to Sprinklr Inc. prior to the order of the Hon'ble High Court of Kerala. No evidence was brought before the Committee of verification of security measures implemented by Sprinklr Inc. The Committee, therefore, is unable to comment on the Privacy, Confidentiality and Security of the data on the basis of the information provided by CDIT.

12.COMMENTS ON PROCEDURES

One of the Terms of Reference of the Committee was to examine whether Adequate Procedures & Processes had been followed while finalizing arrangements with Sprinklr Inc.

The Committee is of the view that the proposal for installing a Digital Platform for analyzing in such a crisis situation, the **Crisis Management** group headed by Chief Secretary should have been activated in which Finance Secretary, Revenue Secretary, Health Secretary, Law Secretary & IT Secretary should have been closely involved. From the files made available to us, it is clear that this Committee headed by the Chief Secretary did not meet during this

47138 1/2020/GAD(AIS-A)

period and discuss the proposal given by Sprinklr Inc. It is learnt that the proposal was not even discussed with Chief Secretary.

As per the rules of business, since Covid-19 is a health issue, the Data Management issues should have been initiated and managed by the Health Department as was done earlier during the Nipah crisis. The Health Secretary, Dr. Rajan.N. Khobragade, IAS, confirmed that there was no formal consultation with the Health Department. We were informed that the Health Secretary had recorded clearly in the file from the IT Department that this was entirely within the purview of the Health Department & IT Department should only play the role of a facilitator. The Health Secretary also mentioned that their Department had developed a similar kind of monitoring system with appropriate MIS which was used effectively during the Nipah Virus outbreak in the State. Similarly, one of the members of the Technical Committee is also stated to have suggested the use of a social media based analytic solution developed by IIITM-K. The Agreement with Sprinklr Inc., since it involves data protection & data security has legal implications. A few of the Clauses concerning data Security and Privacy are highlighted in the previous section. It is opined that therefore before signing the Agreement, the Law Secretary should also have been consulted. There is no evidence on record which suggest such consultation was made with the Legal Department by the Principal Secretary, IT.

Further, in assessing the capability of Sprinklr Inc. to take up the project, a Technical Assessment of the solution by a team of Technical Experts was essential. None of the persons involved in this exercise had the necessary technical expertise in dealing with the subject.

Hence it is clear that there was no team in the IT Department with appropriate knowledge and understanding of such a matter from Techno-Legal viewpoint. Similarly, no person from the IT Department or an external expert was entrusted with the job of monitoring the data that went into the Sprinklr Inc. application software and database system including validation of data security procedures implemented during processing of data and also at the time of transferring data to CDIT computer systems.

On examining the Sprinklr Inc. Agreement, especially the MSA, the Committee was of the view that certain Clauses as mentioned in the Para hereinabove providing omnibus permission to Sprinklr Inc. were not in the interest of the State. By agreeing to the jurisdiction

471386/2020/GAD(AIS-A)

of the US Court, the Kerala Government would not practically, have been able to take any action against Sprinklr Inc. for any infringement and violation in Privacy and Data security of data of Citizens of the State. It may be mentioned that health related data is classified as sensitive personal data. The Data Privacy Bill pending before the Indian Parliament also classifies health related data as sensitive personal information.

Based on our review & examination of the records available with, it appears that due process was not followed by the IT Department in finalizing this contract.

13. FINDINGS AND RECOMMENDATIONS

The Committee has made all efforts to collect, analyze and discuss the findings, confining itself strictly to the Terms of Reference of the Notification of the Government of Kerala.

Based on our review and examination of the records available with us, it appears that a due process was not followed in finalizing this contract by the IT Department.

From the beginning, the case was directly handled by the then Principal Secretary, IT, Mr. M Sivasankar, who followed an ad hoc and unstructured approach. The members of the Technical Committee were not fully in the picture (as has been stated by them). There is no evidence of proper approvals of the competent authorities – in fact, it will not be out of place to mention that proper records have not been maintained. Records of the meetings of the Technical Committee were not drawn up and were not given to the Enquiry Committee despite repeated requests.

The platform was never tested with regard to completeness, efficiency and utility at any point of time after its installation (no documents in this regard were shared with the Inquiry Committee). It may not be out of place to state that the said platform did not find use as was earlier perceived by the Kerala Government. All these issues have been discussed in detail in the earlier paragraphs. Finally, the Committee would like to point out that the approval of the Chief Minister who is also the IT Minister was not taken before the Agreement was executed with Sprinklr Inc. Since we are dealing with data security issues and entrusting sensitive data to a foreign company, this could be detrimental to the interest of the state and its citizens.

471386 /2020/GAD(AIS-A)

The Committee has observed several gaps and weaknesses in the capabilities of the IT Department in its understanding and Selection and Implementation of Data Analytic Digital Platforms. The gaps and weaknesses are related to Technical Skills and Lack of Processes. The digital transformation will employ digital platforms for delivery of services to citizens and data analytics and technologies like AI, machine learning, big data and other Internet-based technologies will be commonly used across disciplines and sectors. Resultantly, privacy and cyber security will pose a stiffer challenge going ahead and the situation will become more complex. It is, therefore, imperative that Kerala overcomes weaknesses and bridges the gaps and focuses on creating skills in Digital Technology and Cyber Security in the State and particularly CDIT and IT Department.
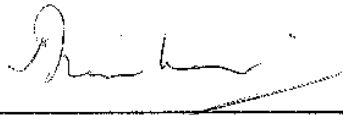
It is recommended that:

1. CDIT and the IT Department must equip themselves to carefully analyze the proposals received from such companies like the case in this report. Had adequate care been used by the IT Department, the latter would have delivered better services to the Kerala Government.

2. The projects are generally of specialized nature and require domain expertise. Therefore, domain specific projects including digital platforms are necessarily implemented by the concerned department rather than IT/CDIT. The latter may only assist the line departments in implementation. It would result in ownership by the concerned Department.

3. The staff of the IT Department and particularly CDIT must be trained in Understanding, Selection, Development and Handling of the Emerging Technologies, Digital Platforms and Cyber Security.

4. Robust and secure ICT infrastructure must be set up for installation of Digital Platforms.

471386 /2020/GAD(AIS-A)

5. Best Practices in respect of Managing and ensuring Security of Digital Platforms be put in place and implemented.

6. Mechanism of checks and balances in implementation and monitoring the security of the digital platforms and the data contained in such platforms should be prescribed and implemented.

7. CDIT must empanel the cyber security auditing companies for audit of the ICT systems of the Kerala government on a regular basis.

8. Memorandum of understanding must be entered with central agencies like STQC, Indian Computer Emergency Response Team (CERT-In) and National Information Infrastructure Protection Centre (NCIIPC). These agencies must be approached for training and skill upgradation of technical staff at CDIT.

Shri M. Madhavan Nambiar   Dr. Gulshan Rai

Chairman   Member

... End of Report

**COMMITTEE CONSTITUTED
VIDE G.O (M.S) NO. 227/2020/GAD DATED 23.11.2020
TO INQUIRE/STUDY IN TO THE ISSUES INVOLVED IN
ENGAGING M/S. SPRINKLR INC. FOR DATA ANALYSIS**

SHRI. K. SASIDHARAN NAIR

FORMER DISTRICT JUDGE AND FORMER SECRETARY
LAW DEPARTMENT
CHAIRMAN

DR. A. VINAYA BABU

RETIRED PROFESSOR, COMPUTER SCIENCE & ENGINEERING
JNTUH COLLEGE OF ENGINEERING, HYDERABAD
MEMBER

DR. SUMESH DIVAKARAN

PROFESSOR, COMPUTER SCIENCE & ENGINEERING
COLLEGE OF ENGINEERING, TRIVANDRUM
MEMBER

**REPORT OF THE COMMITTEE CONSTITUTED FOR
INQUIRING/STUDYING IN TO THE ISSUES INVOLVED IN
ENGAGING M/S. SPRINKLR INC. FOR DATA ANALYSIS**

24 April, 2021

THIRUVANANTHAPURAM

COMMITTEE CONSTITUTED
VIDE G.O (M.S) NO. 227/2020/GAD DATED 23.11.2020
TO INQUIRE/STUDY IN TO THE ISSUES INVOLVED IN
ENGAGING M/S. SPRINKLR INC. FOR DATA ANALYSIS

SHRI. K. SASIDHARAN NAIR
FORMER DISTRICT JUDGE AND FORMER SECRETARY
LAW DEPARTMENT
CHAIRMAN

DR. A. VINAYA BABU
RETIRED PROFESSOR, COMPUTER SCIENCE & ENGINEERING
JNTUH COLLEGE OF ENGINEERING, HYDERABAD
MEMBER

DR. SUMESH DIVAKARAN
PROFESSOR, COMPUTER SCIENCE & ENGINEERING
COLLEGE OF ENGINEERING, TRIVANDRUM
MEMBER

REPORT OF THE COMMITTEE CONSTITUTED FOR
INQUIRING/STUDYING IN TO THE ISSUES INVOLVED IN
ENGAGING M/S. SPRINKLR INC. FOR DATA ANALYSIS

24 April, 2021

THIRUVANANTHAPURAM

INDEX

APPENDICES

Appendix I   1) G.O. (MS) No. 227/2020/GAD dt. 23.11.2020

                                    2) G.O. (MS) No. 63/2021/GAD dt. 25.02.2021

                                    3) G.O. (Rt) No. 512/2021/GAD dt. 03.02.2021

Appendix II   List of Persons called for discussion / inquiry

Appendix III   List of Files, Acts, Ordinances, Rules, Regulations, Instructions, Bills, Reports, Books, Policies referred/relied

Appendix IV   List of documents referred

Appendix V   Cloud Computing, Security and best practices to be followed.

PART - II

ANNEXURES

No.	Subject
Annexure I	Copies of the depositions of persons called for inquiry / recorded video regarding the deposition of Shri. M. Sivasankar, discussions and the proceedings of the Chairman and the copies of minutes of the proceedings of the Committee
Annexure II	Copy of the Report of Shri. M. Madhavan Nambiar Committee
Annexure III	Questions supplied to and replies received from persons / entities
Annexure IV	Copies of documents referred to vide Appendix IV
Annexure V	Copy of the Letter No. 19/2021/Sprinkler dt. 25.03.2021
Annexure VI	Copy of the Letter No. L. 04/CDIT- WSD/2020-22 from C-DIT

MEMORANDUM

Date 24 April, 2021

To

    The Hon'ble Chief Minister of Kerala

From

    Shri. K. Sasidharan Nair

    Chairman

    Dr. A. Vinaya Babu,

    Prof. (Dr.) Sumesh Divakaran,

    Members

Sub   :   Report of the Committee constituted for inquiring/studying in to the issues involved in engaging M/s. Sprinklr Inc. for Data Analysis.

Ref   :   G.O. (M.S) No. 227/2020/GAD dated 23.11.2020

....

The Committee constituted for inquiring / studying in to the issues involved in engaging M/S. Sprinklr Inc. for Data Analysis as per the reference cited, after making an in-depth study on all relevant issues and related aspects, is furnishing the report on this the 24th day of April, 2021.
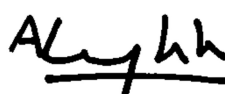
The Committee acknowledges with sincere thanks and gratitude to the Hon'ble Chief Minister of Kerala for the unstinting support given to us for completing our work.

The Committee is also grateful to Shri. K. John Britto, Retd. Special Secretary, Law Department who is engaged as consultant for his contribution and assistance in completing the inquiry/study.

We also place on record our sincere thanks to the staff members of Law Reforms Commission, the officers and staff of the GAD (SS) Section, E&IT Department and the Institutions under the Administrative control of E&IT Department who had given full support and Co-operation in completing the inquiry/study.

K. Sasidharan Nair
Chairman

Dr. A. Vinaya Babu
Member

Prof. (Dr.) Sumesh Divakaran
Member

TERMS OF REFERENCE FOR THE INQUIRY / STUDY

i   Whether the procedure laid down in the Rules of Business of Government of Kerala has been followed while signing the Agreement / Purchase Order?

ii   Whether lapses, which cannot be justified in the extraordinary circumstances prevailing while entering into the Agreement / purchase order, have occurred?

iii   What are and what could have been the measures taken to ensure data security at various periods?

iv   What were the procedures to be followed, apart from those that have been followed, for the Agreement / Purchase Order for obtaining services?

v   Analyse the report submitted by the Committee headed by Shri. M. Madhavan Nambiar

vi   Guidelines to be followed in future.

ABBREVIATIONS

API	Application Programming Interface
C-DIT	Centre for Development of Imaging Technology
CEDA	Centre of Excellence for Data Analysis
CJEU	Court of Justice of the European Union
CSP	Cloud Service Provider
DEPA	Data Empowerment and Protection Architecture
E&IT	Electronics and Information Technology
EC	European Commission
EEA	European Economic Area
EU	European Union
FRT	Facial Recognition Tracking
GDPR	General Data Protection Regulation
GeM	Government e-market place
GOK	Government of Kerala
GSI	Government Secretariat Instructions
IaaS	Infrastructure as a Service
ICFOSS	International Center for Free and Open Source Software
IIITM – K	Indian Institute of Information Technology and Management Kerala
KSUM	Kerala Startup Mission
KSITIL	Kerala State IT Infrastructure Ltd
KSITM	Kerala State IT Mission
LSG	Local Self Government
MeitY	Ministry of Electronics and Information Technology
MOHFW	Ministry of Health and Family Welfare

MSA	Master Services Agreement
MSP	Managed Service Provider
NDHM	National Digital Health Mission
PaaS	Platform as a Service
PDP	Personal Data Protection
PoC	Proof of Capability
Privacy Shield	EV-US Privacy Shield
QCBS	Quality and Cost Based Selection
RFP	Request for Proposal
SaaS	Software as a Service
SCC	Standard Contractual Clauses
SI	System Integrator
SLA	Service Level Agreement
SOM	Secretariat Office Manual
STQC	Standardisation Testing and Quality Certification
US	United States of America
MNDA	Mutual Non-Disclosure Agreement
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
HIPS	Host Intrusion Prevention System
DLP	Data Loss Prevention
IOPS	Input Output Per Seconds
SIEM	Security Information and Event Management
DDoS	Distributed Denial of Service
URL	Uniform Resource Locator
CERT-In	Computer Emergency Response Team- India
SMMS	Sprinklr Social Media Management System
IKM	Information Kerala Mission
TBD	To Be Decided

EXECUTIVE SUMMARY

This report relates to the inquiry/study conducted by a three Member Committee constituted by Government in G.O.(M.S.) No. 227/2020/GAD dt. 23.11.2020, consisting of Shri. K. Sasidharan Nair, Former District Judge and Former Law Secretary, Government of Kerala as Chairman and Dr. Vinaya Babu, Retired Professor, Computer Science and Engineering, JNTUH, College of Engineering, Hyderabad and Dr. Sumesh Divakaran, Professor, Computer Science and Engineering, College of Engineering Trivandrum as expert members to further inquire into the issues involved in engaging M/S. Sprinklr Inc. for data analysis.

2. In the Government Order dated 23.11.2020, Government have stated that the report submitted by Shri. M. Madhavan Nambiar Committee, a two member committee constituted in G.O.(M.S.) No. 79/2020/GAD dt. 20.04.2020 to inquire for the first time into the issues raised in the public domain in connection with the engagement of M/S. Sprinklr Inc. for the purpose of data analysis did not offer its comments on several aspects, especially on legal and administrative aspects in their report.

Therefore this committee was engaged to specifically inquire into the following aspects:

i)   Whether the procedure laid down in the Rules of Business of Government of Kerala has been followed while signing the agreement/purchase order.

ii)   Whether lapses, which cannot be justified in the extra ordinary circumstances prevailing while entering into the Agreement/Purchase order, have occurred?

iii) What are and what could have been the measures taken to ensure data security at various periods?

iv)   What were the procedures to be followed, apart from those that have been followed, for the Agreement/Purchase Orders for obtaining services?

v)   Analyse the report submitted by the Committee headed by Shri. M. Madhavan Nambiar.

vi)   Suggest guidelines to be followed in future.

3.   This Committee has made a detailed evaluation of all materials on record and tried to address specifically the issues involved in the engagement of Sprinklr for data analysis.

4.   This committee at first inquired who was Sprinklr and what was their products and services? The Committee figured out from the

materials supplied that Sprinklr provides a cloud based Software as a Service (SaaS) application provider over the internet. Their services are hosted in a multi-tenant environment and according to Sprinklr, their SaaS model was fundamentally different from other methods of software delivery. Sprinklr operates on a multi-tenant environment that runs the platform for all customers on a "single code line". The platform M/S. Sprinklr typically licensed for a customer was said to be the platform readily available to and already used by over thousands of customers of Sprinklr and when a customer obtains a license, M/S. Sprinklr enables the platform to the customer to provide their services.

5   Sprinklr has specifically stated that the concept of acceptance of this platform does not exist in Sprinklr SaaS business model. According to M/S. Sprinklr, the data collected and processed by Sprinklr in the context of the provision of Sprinklr services for their customers which includes inbound and outbound messages and posts on various social media networks (eg.) Facebook, Twitter etc., for which the Sprinklr's customers who were licensed to use their platform need to authorize M/S. Sprinklr to connect to their social media accounts and allow Sprinklr unilaterally determine the scope of the data collection and processing.

6   Sprinklr has stated that the data collected and processed by them was primarily publically accessible data, in particular social media messages and posts published by the users of various social media networks. Apart from this, it is further stated that Sprinklr collects data provided by their customers using the Sprinklr platform for the purpose of providing the Sprinklr services.

7.   From the materials produced by the E&IT Department and the note of Shri. M. Sivasankar, the then Principal Secretary, it is seen that M/S. Sprinklr Inc. a US based Start-up showed interest in working with Government of Kerala to tackle COVID-19 pandemic and they had the experience of creating user experiences for corporates and had the technology capabilities to pull this fast, the then Principal Secretary, E&IT Department gave a proposal to Sprinklr for using their product capabilities to help the State of Kerala in identifying vulnerable population (to be reverse quarantined) and establishing effective communication channel with reverse quarantined people and engaging with reverse quarantined (suggesting precautions, answering questions, etc.) persons, monitoring their health and reporting geospatially on the health of reverse quarantined in the State and identifying vulnerable persons requiring focussed attention based on insights and engaging accordingly with them.

There upon, the Sprinklr made an offer (Reference 6) expressing readiness to work with the engineers of E&IT Department.

8. It has been stated by Mr. M. Sivasankar that there were discussions in the informal IT support team of which he was the Chairman and the heads of the institutions under the administrative control of E&IT Department as members regarding these issues and based on such discussions and report of the Technical Committee, the Sprinklr was engaged. As per Circular No. DC1/71/2020/LSGD dated 27.03.2020 (Reference 11) a URL, http://kerala-field.covid.sprinklr has been provided with instruction to upload the information of persons in home quarantine in the structured format as per the template appended to that Circular. But even before issuing the above mentioned circular, instructions were given as early as on 20.03.2020 to provide necessary API integration assistance to M/S. Sprinklr Inc. through an e-mail dated 20.03.2020.

9   The Committee is of the view that the capability and other aspects of M/S. Sprinklr was not evaluated and the procedure for engaging such an agency for data analysis, especially sensitive personal data, was not followed in engaging M/S. Sprinklr.

10 This Committee examined the first item of the terms of reference in detail in Chapter II of this report and found that no file was initiated

in the E&IT Department in respect of the engagement of M/S. Sprinklr for data analysis and also that no agreement as required by law was executed between M/S. Sprinklr Inc. and the Government of Kerala (GoK). Thus, the relevant provisions of the Rules of Procedure for the Government of Kerala, the Kerala Secretariat Office Manual and Secretariat Instructions have not been followed by the then Principal Secretary while engaging Sprinklr for data analysis. It is also seen that the Law Department and the Finance Department were not consulted so as to ascertain and confirm regarding execution of agreements and in understanding whether the service offered was cost free.

11   The responsibilities of the Government Department to comply with, especially technical aspects, before procuring the cloud software services, and the non-fulfilment of the same by the E&IT Department in the process of procuring SaaS from M/S. Sprinklr has been discussed in detail in Chapter III of the report as part of addressing the 4th item of the terms of reference.

12   How far the services offered under SaaS by Sprinklr has supported encryption algorithms like AES 256 and higher or whether it comply with P11 data security standards like ISO 27018 are discussed in Chapter III to address item 4 in the Terms of Reference.

13 While attempting to explain what are and what could have been the measures taken to ensure data security at various periods, this committee addressed item III of the terms of reference in Chapter V besides the order of the High Court in WP(C) No. 9498/2020 which sets an important bench mark for all public-private partnerships in the post COVID-19 era in the field of data protection and emphasizes the accountability of the State in handling data of its citizens.

14 In Chapter V, this committee discussed as to whether lapses have occurred while entering in to the agreement/purchase order to address item 4 in the terms of reference. It has also examined whether the lapses occurred cannot be justified in the extra ordinary circumstances prevailing while entering into the agreement.

15 Committee found that there was lapse in having not executed the MSA and SLA. Since E&IT Department was the purchaser department for procuring the cloud services for data analysis from M/S. Sprinklr, the terms and conditions at all-times be construed in accordance with the provisions of I.T. Act, 2000 and the Rules and Regulations issued there under besides the provisions of privacy laws and other applicable laws of India. The MSA format available in the file is not the appropriate format, particularly the provision

regarding jurisdiction fixed in the Federal Courts located in New York City.

16 The SLA had to be prepared incorporating the key service level objectives indicating the measurement methodology to be adopted for measuring the services by defining the target levels and penalties to be levied in case of non-performance. But, only a standard format has been kept in the file as reference (22).

17 Rule 11 of the Rules of Business and Instruction 71 of the Secretariat Instructions say that all orders or instruments made or executed by or on behalf of the Government of the State shall be expressed to be made or executed in the name of the Governor. Rule 11 of the Rules of Business has been incorporated in the Business Rules in compliance of the provision contained in Article 299 (1) of the Constitution of India which are mandatory in character and any contravention there of nullifies the contract and makes the agreement void. But, here the instruments viz. the Order Form and the Mutual Non-Disclosure agreement seen signed by M/S. Sprinklr and Shri. M. Sivasankar have not been executed as required by Rule 11 of Business of the Government of Kerala.

18 On a careful examination of the factual aspects, it is found that Shri. M. Sivasankar who was the then Principal Secretary of E&IT Department was wholly responsible for the engagement of Sprinklr

Inc. for data analysis. Before engaging Sprinklr, he should have initiated a file and processed the same as required by law. He should have consulted the High Power Committee headed by the Chief Secretary, he should have duly informed the Hon'ble Chief Minister who was the Minister in charge of E&IT Department regarding the engagement of Sprinklr, he should have seen that necessary agreements are executed in appropriate formats, he should have ensured proper data security for the reason that sensitive data was being uploaded to the URL provided by Sprinklr, he should have consulted the Law Department to confirm proper execution of agreements, he should have consulted Finance Department to ascertain whether there was financial implications, there should have been formal consultation with the Secretary, Heath Department being the implementing department and also the Secretary, LSGD for the reason that the details in the template appended to the Circular dated 27.03.2020 were being collected by the field staff of that Department. But instead, he is found to have preceded on the wrong premises that he as the head of E&IT Department was purchasing a product having financial implication of less than Rs. 15,000 and so only Store Purchase Manual was needed to be followed and thus issued the purchase order (Reference 21) after having engaged Sprinklr for data analysis.

19   On a totality of all facts and materials on record and taking note of the extra-ordinary circumstances prevailing at that point of time, the Committee is of the view that no evil design, malice or bad faith can be attributed upon Shri. M. Sivasankar for his lapses in engaging Sprinklr for data analysis. The Sprinklr activities continued only for less than a month and by 20.04.2020, the entire data has already been transferred to the State Data Centre managed by C-DIT and instructions was also given to destroy data if any remained with Sprinklr forthwith. Accordingly Sprinklr reported compliance with the same. There is no evidence, as of now, to prove that the interest of the State was adversely affected due to the engagement of Sprinklr. The above aspects have been discussed in Chapter V of the report.

20   The analysis of the report submitted by the Committee headed by Shri. M. Madhavan Nambiar is the fifth item of the Terms of Reference and the same has been discussed briefly in Chapter VI of the report.

21   In Chapter VII this Committee has given few recommendations and guidelines to be followed in future.

List of Persons called for discussion / inquiry

Sl.No.	Name	Designation
1	Smt. Archana C.S.	Assistant (B1) E&IT Department
2	Shri. Manesh Mohan	SO, E&IT (B) Department
3	Shri. Vinod G.	Addl. Secretary, E&IT Department
4	Dr. Divya V.S.	State Nodal Officer (Training), National Health Mission
5	Shri. Biju S.B.	Head of Department, Web Services, C-DIT
6	Dr. Sabareesh	Head, E-Governance, KSITM
7	Dr. Jayasankar Prasad C.	Managing Director, KSITIL
8	Shri. R.S. Kannan	Special Secretary, Local Self Government Department
9	Dr. Saji Gopinath	Vice Chancellor, K.U.D.S
10	Shri. Neelakantan D.S.	Deputy Director (Technical), IKM
11	Shri. Sasi P.M.	CEO, Technopark, Thiruvananthapuram
12	Dr. Chithra IAS	Director, KSITM, Director, C-DIT, Director, IKM, Director, Training Directorate of Industrial Training
13	Shri. M. Sivasankar	Former Principal Secretary, E&IT Department

List of Files, Acts, Ordinance, Rules, Regulations, Instructions, Bills, Reports, Books, Policies referred/relied

No.	Documents
1.	File No. I.T.B1/16/2020 – ITD (Computer No. 1480105)
2.	File No. I.T.B1/25/2020-ITD (Computer No. 1492042)
3.	File No. I.T.B1/25/2020-ITD Part (1) (Computer No. 1494156)
4.	File No. I.T.B1/25/2020- ITD Part (2) (Computer No. 1496986)
5.	File No. T.T.B1/25/2020- ITD Part (3) (Computer No. 1497826)
6.	File No. I.T.B1/26/2020 – ITD (Computer No. 1531974)
7.	File No. ITB1/139/2020-ITD (Computer No. 1635621)
8.	Information Technology Act, 2000
9.	The Contract Act, 1872
10.	Indian Telegraph Act, 1885
11.	Disaster Management Act, 2005
12.	The Aadhaar (Targeted Delivery of Financial and other subsidies, benefits and services) Act, 2016 (Act 18 of 2016)
13.	The Census Act, 1948 (Act 37 of 1948)
14.	The Aadhaar and other laws (Amendment) Act, 2019 (Act 14 of 2019)
15.	Kerala Epidemic Disease Ordinance 2020 (Ordinance No. 18 of 2020)
16.	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011)

17.	Constitution of India
18.	DNA Technology (use and application) Regulation Bill, 2019 Bill No. 142 – C of 2018
19.	The Personal Data Protection Bill, 2006
20.	The Personal Data Protection Bill, 2019
21.	The Store Purchase Manual, and Budget Manual
22.	The Kerala Secretariat Office Manual
23.	Sreekrishna Committee Report
24.	Administration Reports of E&IT Department and institutions under E&IT
25.	Report of Mr. Kris Gopalakrishnan on Non-personal Data Governance Framework.
26.	Kerala Government Secretariat Instructions
27.	Handbook on delegation of powers to the officers of the Secretariat
28.	Rules of Business of Government of Kerala
29.	National Digital Communications Policy, 2018
30.	Draft National e-commerce policy
31.	Agency Master Service Agreements/Master Service Agreements of Sprinklr, different versions and different countries.
32.	Data Protection Act, 1998, U.K.
33.	State Records Act, 1997 (No. 8 of 1997) South Australia
34.	I.T. Policy of Government of Kerala and other States
35.	Indian Conveyancer by Mogha.

LIST OF DOCUMENTS

No.	List of documents referred
1	G.O. (M.S) No. 79/2020/GAD dt. 20.04.2020
2	Reference (11) – Circular No. D.C 1/71/2020/LSGD dt. 27.03.2020
3	Reference (22) – Service Level Agreement
4	Reference (21) – Order Form
5	Reference (23) – Master Service Agreement
6	Reference (24) – SMMS Privacy Policy
7	Reference (25) – Acceptable User Policy (AUP)
8	Reference (33) – Mutual Non-Disclosure Agreement
9	Reference (6) – E-mail dt. 20.03.2020 from Ragy Thomas
10	Reference (5) – Digital Contagion Management Solution

Cloud Computing, Security and best practices to be followed:

In this appendix, we report the best practises recommended for adopting a cloud service. The first section discusses cloud computing, cloud computing models and different types of cloud services. Security aspects of cloud computing is presented in the second section. Third section talks about security concerns regarding sensitive data when an organisation utilises the service of a third party to develop a Machine Learning/Artificial Intelligence application. Finally, the last section shows the best practises recommended for adopting cloud services with necessary provisions to ensure security of sensitive data.

We use a running example in this section to introduce the concept of cloud computing, various cloud computing models & services and Machine Learning (ML)/Artificial Intelligence(AI) based software solutions. Let us consider the following problem. Let $\mathcal{D}_{CP}$ be a dataset containing required information about the COVD 19 positive cases in a State and $\mathcal{D}_{SC}$ be a dataset containing required information about Senior Citizens in the State. We have to find those senior citizens who are susceptible to be infected by Corona Virus due to direct or indirect contact with people whose data is included in $\mathcal{D}_{CP}$.

Suppose $\mathcal{S}$ is an application software to solve the above problem. $\mathcal{S}$ needs to find required inferences from the dataset $\mathcal{D}_{CP}$ and $\mathcal{D}_{SC}$, may be based on the travel history for which it needs to use some ML/AI algorithms. Now, we need a computing infrastructure to execute/run $\mathcal{S}$ on $\mathcal{D}_{CP}$ and $\mathcal{D}_{SC}$.
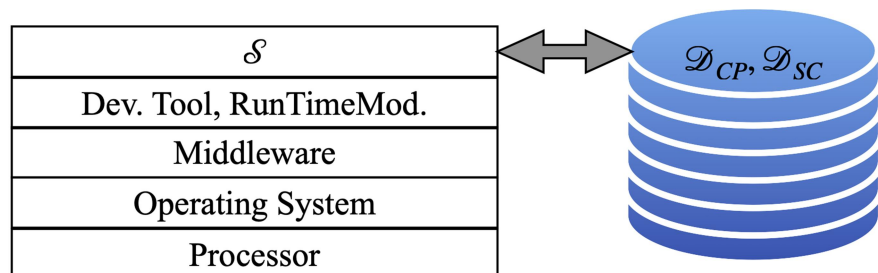
The compute infrastructure includes a Processor which is the hardware on which S can be executed with the help of intermediate softwares as shown by the above layered architecture. An organisation should have this compute infrastructure to utilise S for solving a problem like the above. The main resources of a computing infrastructure to be consumed by S is the time of the processor and storage space required to hold $\mathcal{D}_{CP}$ and $\mathcal{D}_{SC}$.

Cloud Computing

Cloud computing is a concept where the compute infrastructure required by an organisation for a computing purpose can be accessed from the internet using a program called a web browser. When we use a cloud service network becomes another important resource to be consumed by a program like S. A company which provides the compute infrastructure is called the Cloud Service Provider (CSP). A cloud computing model defines how the cloud service is implemented and who can access the infrastructure. There are basically four types of cloud computing models.

1. **Public Cloud**

This is a cloud system where a number of organisations (called **tenants**) share the same set of compute resources. Main advantage of this cloud system are scalability (resource usage can be changed dynamically) and small capital investment. The main drawback is the difficulty in ensuing security of sensitive data since multiple tenants are sharing the compute devise the and storage.

2. **Private Cloud**

This is a cloud system where the required compute infrastructure is exclusively earmarked for a single organisation and hence no entity outside the organisation gets access to the cloud system. The main advantage of this cloud system is the security of data stored on the cloud. The main disadvantages are huge capital investment and the issues with scalability.

3. **Hybrid Cloud**

This is a cloud system which is basically a combination of public and private cloud. In this model, typically an organisation can maintain the sensitive data and its processing in a private cloud and rest can be hosted on a public

cloud. With proper planning, required security can be ensured on a hybrid cloud without a huge capital investment, when compared to the private cloud.

4. **Community Cloud**

This is a cloud system where multiple tenants of a community share the same set of compute resources. For example, a Country can have a Government Community Cloud where different Government Organisations share a set of compute resources. It is cost effective since, the capital investment can be shared by various Government Organisations. It is more secure when compared to the public cloud since, only Government entities get access to the resources.

There are three basic types of cloud services. They are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These can be depicted as a pyramid.
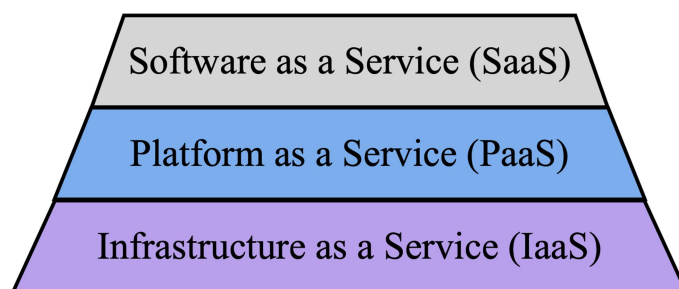
1. **Infrastructure as a Service (IaaS)**

This is the most general type of cloud service available. In this, the CSP just provides the processor and storage on the internet. The tenant can purchase/develop and maintain Operating System, Middleware, Development Tools, Run Time Modules and Applications Softwares. Thus the tenant can have full control on the system except the processor and storage which are managed by the CSP. A tenant shall verify that necessary provisions are included in the Service Level Agreement to ensure that required level of security is provided by the CSP to prevent authorised access to its sensitive data while it is stored and processed in the cloud. Example CSPs proving IaaS include Amazon Web Service (AWS), Google Compute Engine (GCE) and Microsoft Azure.

2. Platform as a Service (PaaS)

This is a type of cloud service which extends IaaS by providing Operating System, Middleware, Development Tools and Run Time Modules. Here the tenant can develop/purchase Application Softwares. Service Level Agreement in this case shall cover the required provisions to ensure that necessary security measures are provided by the CSP to prevent unauthorised access to its sensitive data in any means from the infrastructure provided by the CSP. Here, everything except the application software is completely managed by the CSP.

3. Software as a Service (SaaS)

This is a specialised type of cloud service which provides the required application softwares over PaaS. In this case, everything is managed by the CSP. It is very important that the tenant and the CSP have a clear picture about the functionality to be provided by the application softwares. The Service Level Agreement/Master Service Agreement shall include functionality to be provided by the application softwares, efficiency requirements, security measures required to prevent unauthorised access to sensitive data and provisions to ensure that the CSP is responsible to provide required training to the tenant manpower regarding the use of application softwares. This type of service is advisable for organisations which do not have competent manpower to develop and maintain required application softwares.

Security in Cloud Computing

Cloud computing environment makes data security and privacy a major concern, since an organisation's data will be stored and processed outside its premises and control. While collecting, transporting, storing or processing sensitive data, the system should ensure the value, integrity, confidentiality and availability of sensitive data involved. For this, the system should ensure that unauthorised access, misuse, improper disclosure or destruction is not allowed on sensitive data.

Any laxity which leads to leakage of sensitive data like health-related data, biometric data of people, Name, Mobile Number and Address of people, political/religious inclination of people etc. can lead to serious consequential

impacts. The union Government has introduced THE PERSONAL DATA PROTECTION BILL, 2019 to protect the privacy of individuals relating to their personal data. Measures need to be incorporated to ensure that these acts are respected while using a cloud service. Required mechanisms should be provided to safeguard the organisation's data. The mechanism should be enough to ensure that:

(i) **Data integrity is preserved**. Unauthorised data modification should be prevented when data is transmitted over internet, kept in the cloud storage and processed in the cloud compute device.

(ii) **Confidentiality of data is not compromised**. Unauthorised data access should be prevented when data is transmitted over internet, kept in the cloud storage and processed in the cloud compute device.

(iii) **Data availability not affected**. Denial of service due to any cause needs to be prevented. Proper back-up and disaster recovery plans should be implemented to ensure continuous availability of service, without being affected by loss of data due to any type of possible failures of functioning of the cloud system.

(iv) **Consent from individual is taken**. While collecting personal data each individual must be informed about the purpose of collecting data, where is it stored & processed and who all gets access to it and for what purpose such entities shall be given access.

(v) **Personally Identifiable Information (PII) is masked**. When data access needs to be provided for a third party like software developers PII need to be masked. Techniques like removal, encryption, aggregation, anonymization, pseudonymization etc can be used to mask data depending on the purpose for which the data have to be shared.

(vi) **Application log and database log are maintained**. Logs are like a blackbox for an aircraft. Even in the instance of application softwares and databases are lost due to some type of hardware/software failures in the cloud platform, logs should be safely maintained by using an appropriate technology like keeping multiple copies of logs at different geometrical locations. Application log can be analysed to see the details of who all have accessed the application software

and database log can be analysed to determine the details of who all accessed the content of database. Proper plans should be implemented to keep application and database logs until these are analysed to verify that unauthorised accesses are not happened to the application softwares and databases on the cloud system.

Selecting an appropriate cloud computing model is very crucial to ensure required security. Private cloud system can provide maximum security since the infrastructure (compute device, storage and network) provided to an organisation is not accessible to any other organisation. But, it has the disadvantage of requiring huge capital investment as the entire cost of the required infrastructure needs to be met by the organisation alone. A hybrid cloud system where a private could in the premises of the organisation to store and process sensitive data and to use a public cloud to store and process the remaining data may be a good choice. Another option is to use a Community Cloud where only entities in the community gets access to the infrastructure. For example, it is advisable for various Government Institutions to share a community cloud service. However, an organisation shall have a properly planned data access policy and accordingly, a fine-grained role-based access control mechanism should be made in place to ensure that only responsible employees of the organisation are allowed to access data and that data access is regularly monitored to verify that data access policy of the organisation is not violated.

Planning proper mechanisms to deal with common security concerns on cloud system is very important. We list below the typical security concerns on cloud systems.

(i) **Data Breach**. An action which steals or accesses data from the cloud without the knowledge or authorisation of the owner of the data.

(ii) **Improper Cloud Account Management**. Any type of actions through which an attacker hijacks the access credentials (Username and Password) of an existing cloud account shall lead to unauthorised access/modification of sensitive data on cloud.

(iii) **Insider Threat**. Employees of the organisation who has cloud account user credentials misusing the account to steal sensitive data stored on the cloud.

(iv) **Regulatory Compliance**. Data which is considered as sensitive in one Country may not be considered as sensitive in another Country. Hence, deciding law jurisdiction is very important when adopting a cloud service.

(v) **Insecure Application Programming Interfaces** (APIs). APIs may be provided to customise a cloud platform. They provide means for different application softwares to interact. But, improper usage of APIs may cause security violations. Provisions should be incorporated to ensure that only those users authenticated with required access privilege are allowed to access such APIs. The security requirement on a cloud system may demand encryption/masking of the data to be transmitted over the internet. Then, special care should be taken to ensure that data shared via APIs between two application softwares is also encrypted or masked.

(vi) **Denial of service attack**. Any type of actions by malicious agents on the internet which prevent legitimate users of the cloud system from getting the expected services. For example, an attacker may overload the network by sending lot of packets (unit of data transmitted over a computer network) to cause network congestion thereby causing nonavailability of service on time.

(vii) **Insufficient Due Diligence**. Lack of proper planning and implementation regarding the type of cloud computing model and cloud service to be adopted, security measures to be incorporated, account management strategy, assigning role-based access privileges and monitoring access control can lead to security violations.

(viii) **Shared Responsibility**. Ensuring security in cloud systems is a mutual responsibility of the CSP and the tenant. Security requirements must be clearly listed and included in the Service Level Agreement. Both parties should ensure that the security requirements are respected during the development, deployment and maintenance of the cloud system.

(ix) **Data Loss**. Data stored in the cloud system can be lost due to various reasons such as natural disaster, hardwire/software failures, intentional or unintentional

deletion of data by application softwares, attacks from a malicious agents on the internet etc.

Ensuring data security when using a Machine Learning (ML) application

Cloud systems which need an ML application to provide a SaaS may need to access data for training the required ML engine (software to find inferences from data). For example, consider the application introduced in the preface part of this chapter. An ML application to find the required inferences needs to be trained with enough data from the datasets $\mathcal{D}_{CP}$ and $\mathcal{D}_{SC}$. This may compromise the security requirements since application developer (CSP) needs access to data. One approach for providing security is removing sensitive data before dataset is made accessible to the CSP for the training purpose. But, a difficult question to answer is what we do if it is essential for an ML training to use sensitive data? There are some techniques proposed in the literature to mask sensitive data required for training an ML engine. But, any types of transformations applied on data to mask it may adversely affect the functioning of an ML application to find the required inference. So the organisation has to take an appropriate decision regarding disclosure of sensitive data. It is not easy to solve this dilemma. A compromise should be made between security implications and precision in the inference required, and in such cases expert opinions should be taken from both legal and technical experts to take an appropriate decision. Anyhow, personal sensitive data should not be disclosed to a third party without informed consent from the persons involved. Also, stringent provisions should be added in the Service Level Agreement regarding the use of access on sensitive data, to the effect that the CSP is not allowed to use the data for any purpose other than using it for training the ML engine.

Dealing with security needs identification of sensitive data as the first step. Once sensitive data is identified, the next step is to plan strategies to prevent misuse of sensitive data without adversely affecting the application to be developed. Most common approaches used to secure sensitive data are - removing sensitive data, masking sensitive data and coarsening sensitive data.

The first step is to identify sensitive data which may occur in various forms:

(i) **Sensitive data in columns**. In this case the sensitive data may be a subset of columns in a database table. For example, the attributes Name, Mobile Number and Email Address of a personal database table may be identified as sensitive data. It is easy to identify sensitive data of this kind.

(ii) **Sensitive data in unstructured text-based dataset**. Sensitive data may be present in unstructured text-based dataset. For example, personally identifiable information shared over a social media network may be sensitive, which needs to be protected from unauthorised access. There are techniques like regular expression based pattern matching which can be used to identify sensitive data of this kind.

(iii) **Sensitive data in free-from unstructured dataset**. Sensitive data can be present in unstructured data formats such as audio files, video files, images and scanned files. It is more difficult to identify sensitive data in these cases. However, various approaches are proposed to deal with each case. Audio files may be first covered into text files using a speech-to-text transformation software and then use some of the techniques such as natural language processing or regular expression based pattern matching to identify sensitive data from the obtained text files. Various image processing tools can be used to identify sensitive data contained in images. For video files, one may use video processing tools or first covert the video into a sequence of images and then use techniques for identifying sensitive data from images.

Now we discuss the common approaches used to secure sensitive data when data access need to be provided to the CSP for training an ML engine.

(i) **Removing sensitive data**. If sensitive data is not essential for training, then it can be removed from the dataset before the dataset is given to the CSP. If sensitive data is a subset of columns in database tables, then creating views without the columns comprising the sensitive data can be given to the CSP. In cases of sensitive data present in text-based data set and when it is identified using regular expression based pattern matching, then similar pattern matching approaches can be used to remove such data. In the case of sensitive data

present in free-form structured data, appropriate techniques need to be used to remove sensitive data.

(ii) **Masking sensitive data**. When it is essential to use sensitive data for training an effective ML engine, we cannot remove such data. Then, we have to apply some techniques to mask such data, provided the ML engine can be effectively trained using the data in the masked form. There are various masking techniques:

(a) One approach is to *encrypt* sensitive data using an acceptable encryption algorithm. In this case, cypher text (transformed data from which the CSP cannot reproduce the original data) can be given to the CSP instead of giving plain text.

(b) *Tokenisation* is another masking technique where a real value in a sensitive data will be replaced with a dummy value. For example, real value in a PAN card number can be replaced with a dummy value which will make it difficult for the CSP to reproduce the original PAN card number of a person. It is necessary for an ML dataset that the same dummy value must be used to replace all occurrences of a real value in the dataset.

(c) *Dimension reduction techniques* such as Principal Component Analysis (PCA) can be used to mask data. In this case several attributes will be combined into PCA vectors. This will make it difficult for the CSP to reproduce the actual attribute values in the dataset.

(iii) **Coarsening sensitive data**. This is a technique to decrease the precision or granularity of sensitive data to make it difficult for the CSP to reproduce the sensitive data. The following are the data fields which are well suited for applying this technique.

(a) **Locations**. Population density of a particular category of people is a sensitive data of high demand. Rounding off location coordinates in the addresses of locations can be used to hide the exact details from this data. But, it is difficult to identify how much one should round-off to make it difficult to identify the exact population density of a category of people. When rounding is not sufficient to mask, one can use location identifiers such as city, state or pin code which

makes it difficult to identify the location of an individual, since it represents a larger area where a lot of people are located.

(b) **Pin codes**. Pin codes can be coarsened to include a subset of the 6 digits.

(c) **Numeric Quantities**. Numeric quantities can be coarsened by including ranges instead of giving the exact numeric value. For example, age may be replaced by an interval of ages say form 40 years to 60 years. Another example of coarsening is replacing the birth date of a person with the month or year of birth.

(d) **IP Addresses**. Widespread use of internet in daily life makes the IP address of a person as sensitive as her/his physical address. An IP address is composed of a group of numeric fields. An example coarsening for an IP address is to replace one numeric field with zeros.

Even though there are such approaches proposed to mask/hide data, sometimes we may require to provide row data for training an ML engine to get an effective ML application. If such data are identified as sensitive, then an appropriate decision should be taken for each such case based on expert opinions to be obtained from competent legal and technical experts.

Why should a Government Department adopt a cloud service ?

A Government Department may have to utilise cloud service for various reasons including the following:

(i) Capital investment can be significantly reduced since the charges for using a cloud service is much lesser when compared to the investment required for the purchase and maintenance of the required IT infrastructure.

(ii) Lack of trained manpower with working knowledge in maintaining a data centre and compute server.

(iii) Cloud infrastructure is regularly updated with the recent development in technology and hence use of cloud service enables a Government Organisation to enjoy the benefits of an efficient software application which needs to use the recent technological advancements.

(iv) Cloud Service Providers have more competent manpower and mechanisms to ensure security and reliability of service when compared to a Government

system. A proper plan for adopting a cloud service with necessary conditions included in the Service Level Agreement can ensure more reliable and secure operation on cloud.

(v) Scalability of a cloud system is much better than the conventional system. Selecting a suitable cloud computing model enables to maintain an easily scalable system with a lesser cost.

However, proper planning, implementation and monitoring is very important for a Government organisation for adopting a cloud service. In this section, we report the best practises recommended to be followed while adopting a cloud service. The E&ITD shall maintain a Technical Expert Team (TET) comprising of regular employees of the department with necessary qualifications and competency to help Government Departments in preparing an effective plan for adopting a cloud service.

(1) **Deciding whether to go for a cloud service**.

The first step is to decide whether the Government Institution needs a cloud service or a software which can be hosted on the state data centre. TET shall be entrusted to study this and list the pros and cons in each case. Based on the report of the TET, a decision has to be taken by the Government depending on which is more valuable for the Government.

(2) **Deciding a cloud computing model**.

There are basically four cloud computing models. They are - Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud. Each has its own merits and demerits. A Hybrid cloud model where the sensitive data is stored and processed in a private cloud maintained by the Government in it premises and using public cloud for the rest, or a Government Community Cloud may be ideal for a Government Organisation. Nonetheless, expert opinion from TET shall be obtained before deciding a cloud model.

(3) **Deciding a cloud service**.

There are basically three types cloud services. They are - Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Another cloud service which is recently introduced is Function as a Service (FaaS). Depending on the application and the manpower available

with the Government Institution, an appropriate cloud service should be decided by the Government based on the expert opinion to be provided by the TET regarding the pros and cons of each type of service for the application for which the Government Institution needs a cloud service.

We list below the important steps to be followed to ensure security of sensitive data while adopting any type of cloud services.

(a) **Identify sensitive data**. The first step in ensuring security of sensitive data is the process of identifying sensitive data involved.

(b) **Ensure data integrity**. The objective here is to prevent authorised and unintended modification of data. The following measures are recommended for ensuring data integrity.

(i) Mechanisms like hash value checking at regular intervals shall be done by the application software to ensure that stored data is not tampered by malicious users.

(ii) Proper planning should be there to decide roles and privileges of employees to ensure that only responsible employees are given modification privilege on data.

(iii) APIs if any are provided must be carefully designed so that only authenticated users with modification access privilege are allowed to execute the APIs modifying data.

(iv) Application software shall include a monitor to identify and report attempts from unauthorised agents to access data. Techniques like IP whitelisting and AI/ML algorithms may be used to implement this.

(v) Ensure enforcement of proper cloud account management policy.

(vi) Ensure that law jurisdiction is within the Country in case of any data breach reported.

(vii) Ensure that data is stored physically within the country.

(c) **Ensure confidentiality of sensitive data**. The objective is to prevent authorised access of data. Sensitive personal data should not be made accessible to a third party without informed consent from the persons involved. The following measures are recommended for ensuring confidentiality of sensitive data.

(i)   Decide and implement fine grained role based access control and ensure that only authenticated users are getting access to the data stored, transmitted over internet and processed.

(ii)   Ensure that sensitive data is encrypted when it is transmitted over internet and when it is stored and processed on the cloud.

(iii) Ensure that only authenticated users are accessing the application software.

(iv)   Ensure data security at run time.

(v)   Ensure that use of APIs to enable customisation of the cloud is not compromising the confidentiality of sensitive data.

(vi)   Ensure that personally identifiable information is masked before third party access is enabled on a dataset.

(vii) Ensure that application log and database log are maintained until they are analysed to verify whether unauthorised access to application or data is happened. It is advisable to implement a monitor which regularly analyses the log files. Special care should be taken to ensure that only the administrator has privilege to run the monitor. If monitor is not implemented, then ensure that the log files are analysed in regular intervals.

(viii) Ensure enforcement of proper cloud account management policy.

(ix)   Ensure that law jurisdiction is within the Country in case of any data breach reported.

(x)   Ensure that data is stored physically within the country.

(xi)   Ensure that sensitive data is masked before access to dataset is enabled to a third party even when the third party wants to use the data for training an ML engine. If the ML application requires access to row data for the training purpose, then expert opinions from legal and technical experts should be taken and an appropriate decision should be taken by the Government. Nevertheless, sensitive personal data should not be made accessible to a third party without informed consent form the parties concerned.

(d) **Ensure availability of data**. The objective is to make sure that legitimate users of the system are getting uninterrupted access to the data stored on the cloud. Preventing data loss and mechanism to recover lost data if any is required. There are various chances for data loss on a cloud system including hardware/software failures, unintentional data deletion by the application software, data deletion by malicious agents on the internet, natural calamities etc. Required backup and recovery mechanism shall be provided to ensure uninterrupted data access to legitimate users.

CHAPTER – 1

INTRODUCTION

1.1   India is transforming in to a digital society. While transition to a digital economy is underway, the process of personal data has already become omnipresent. The reality of the digital environment today is that almost every single activity undertaken by an individual involves some sort of data transaction or the other.

1.2   While data can be put to beneficial use, the unregulated and arbitrary use of data, especially personal data, has raised concerns regarding the privacy and autonomy of individuals.

1.3   This was also the subject matter of the landmark judgment of the Supreme Court in Justice K.S. Puttaswamy (Rtd.) & another Vs Union of India & others (W.P.(C) No. 494 of 2012) which recognized the right to privacy as a fundamental right.

1.4   The Kerala High Court in Balu Gopalakrishnan V State of Kerala (WP (C) NO 9498/2020) passed an interim order on 24th April, 2020 on the export of COVID-19 related data by State

Government to a US based entity, M/S. Sprinklr Inc. for data analysis. This order sets an important bench mark for all public, private partnerships in the post COVID-19 era in the field of data protection and emphasizes the accountability of the State in handling data of its citizens.

1.5   Need for inquiry/Study of this committee.

Government in G.O. (M.S) No. 227/2020 dt 23.11.2020 have stated that a detailed examination by experts in legal, administration and Information Technology domain was required on many aspects on which the earlier committee has not offered its comments in their report and therefore appointed this three members committee to inquire in to the specific aspects on the terms specified there in.

1.6   Commencement of the work

The three Member committee constituted by Government took charge on the FN of 03.12.2020 in the first meeting convened through video conferencing. The Committee used the infrastructure, office space and staff available at the office of the Law Reforms Commission vide G.O.(Rt) No. 512/2021/GAD dated 03.02.2021.

1.7 Scope of Inquiry/Study

This Committee confined its inquiry/study on the specific questions found in the terms of reference. The Committee inquired about Sprinklr and their products and services and what kind of data Sprinklr was processing in its platform and whether the data protection regime was in compliance with GDPR, the procedure undertaken in the E & IT Department for the engagement of Sprinklr, the guidelines to be followed for procuring cloud software service from a CSP for Government Departments and the security practices and procedures to be followed in the procurement of Cloud Software Services. We also have looked into the data security issues addressed by various Courts in our country and the provisions in the IT Act 2000 in respect of data security measures adopted by Government and regarding the writ petitions filed before the Honourable High Court alleging breach of protection of personal data in the engagement of Sprinklr.

Apart from this, the IT institutions working under the administrate control of E & IT Department was also inquired.

1.8 Source and Method

Depositions of persons examined, discussions in virtual meetings, materials received from the files, documents and records received from E&IT, GAD and other institutions under the administrative control of E&IT, the acts and guidelines governing data security

and Information Technology, Constitution of India, Government Secretariat Office Manual, Secretariat Instructions and Rules of Business of Government of Kerala were referred and relied.

1.9 At first, the file No. IT (B1) 16/2020/ITD and the report of Shri. M.Madhavan Nambiar Committee forwarded from the Administrative Department (General Administrative Department) were examined. The committee then called for and received certain other files, records and cases relating to Sprinklr engagement and they were examined. There after the Committee forwarded specific questions to M/S. Sprinklr Inc., E&IT Department, and to the Institutions coming under the administrative control of E&IT and the answers received were perused. Then the committee identified the persons to be examined and on appearance, their depositions were recorded. A virtual meeting was conducted and Shri. M. Sivasankar was heard. Then, the committee made an in depth study of the entire materials, evidences and also considered the relevant laws on the issues and accordingly prepared this report.

1.10 It is learned from the log audit reports that data got recorded to the database incorporated with the SaaS application with effect from 25.03.2020. But, the application logs provided to the audit agencies by C-DIT is from 03.04.2020 only. Therefore, the committee wanted to know the reason for C-DIT to not provide the application logs from 25.03.2020 to 03.04.2020. Accordingly, the committee contacted C-DIT, AWS and M/S. Sprinklr Inc. through

E&ITD, GoK vide letters in annexures V and VI to obtain the reason for the same. Response is not received on these either from AWS or from M/S. Sprinklr till 24.04.2021, the date of finalising this report. However, C-DIT has submitted a reply in which they stated that when C-DIT asked about the same, Sprinklr had informed C-DIT that the application logs recorded till 03.04.2020 were automatically overwritten by the system, since they had configured the system to overwrite the log files when its total size exceeds a limit. Hence, the Committee is not in a position to comment about the unauthorised access if any happened on the SaaS application during this period.

1.11 However, the log analysis and Assessment Report of Sprinklr application platform conducted by a CERT-In empaneled audit agency in their report dated 17.05.2020 has categorically stated that during their assessment they found that there was no unauthorised access been identified and there was no sign of data leakage or breach happened on the Sprinklr application during the logged period. (April 3rd 2020 to April 19th 2020)

CHAPTER – II

Whether the procedure laid down in the Rules of Business of Government of Kerala has been followed while signing the Agreement/purchase order (Item No. 1 in the Terms of Reference)

2.1   While considering this term of reference, it would be proper and appropriate to give a brief description about the Secretariat Organisation, the course of action on a paper from receipt to disposal in Government, how cases are dealt with in the Government Secretariat with noting procedures and the departmental disposal of business in Government.

2.2   The Rules of Business of the Government of Kerala have been made by the Governor of Kerala in exercise of the powers conferred under clauses 2 and 3 of Article 166 of the Constitution of India. As per Rule 4, the Business of the Government shall be transacted in the Department specified in the First Schedule and shall be classified and distributed between those departments as laid down there in. Sl.No. XIX of the first schedule is Information Technology Department, later renamed as Electronics and Information Technology Department, (for short E&IT Dept.)

Formulation of policies relating to Information Technology and their implementation come under item 1 and co-ordination of Government initiatives comes under item 2 of this department. The issues involved here in come under the above items and so the E&IT Department was competent to deal with this subject.

2.3 The Secretariat is mainly concerned in assisting the Cabinet in framing of policies, approval of plans, programmes and activities for the overall development of the State, the work connected with Legislation, laying down rules and proceedings, financial control, general direction and monitoring and evaluating the work done by the implementing departments/agencies.

2.4 The business of the Government is transacted through various Secretariat Departments. The said business is classified and distributed between the departments of the Secretariat in the manner specified in the First Schedule to the Rules of Business of the Government of Kerala. Each Department of the Secretariat consists of a Secretary to Government who is the official head of the Department.

2.5 The Secretary is responsible for the careful observance of the Rules of business and the Secretariat Instructions in the transaction of business in his Department.

2.6   Incoming papers in the Departments are received by the office
        section. In addition, communications addressed in the name of
        officers and those received by the offices of the Chief Minister and
        other Ministers are given to the respective Departments for
        processing.

2.7   After registering the papers they are processed by the Assistant.
        The initial step is to find out whether they relate to any of the
        pending files. If so, they are added to the concerned file and
        further action taken. In other cases they are treated as fresh
        cases and new files are opened.

2.8   In cases where Finance, Law or Personal and Administrative
        Reforms Department or any other Secretariat Department has to
        be consulted under the Rules of Business/Secretariat instructions,
        the file shall be referred to that department.

2.9   Once a decision is taken on the file and if required to be
        communicated, it is done in the form of a Government Order,
        notification, letter or any other approved form of correspondence.

2.10   When in the course of dealing with a subject, any fresh subject
        arises which it is desirable to deal with separately, extracts should
        be taken of the parts of the current file and note file relating to the
        fresh subject and with these a separate file should be started. A

note should be made in the note of the main file to the effect that a fresh file has been opened and its current number should also be noted. This will probably be necessary whenever the original title of the current file no longer correctly describes the actual subject under correspondence and not otherwise (SOM 102).

2.11 Inter-departmental references of files become necessary when the proposal requires clearances, concurrence, advice or opinion of other departments or sections as required by the Rules of Business or the Secretariat Instructions (SOM 104).

2.12 In respect of matters affecting the finances of the State as classified from time to time in the Rules of Business, Finance Department shall be consulted except where specific delegations are given to the Administrative Department under Rule 10(i) of the Rules of Business (SOM 109).

2.13 Rule 10(i) says that no department shall without previous consultation with finance department, authorise any orders (other than orders pursuant to any general delegations made by the Finance Department), which, either immediately or by their repercussions, will affect the finances of the State. Apart from this, there are situations requiring consultation with Finance

Department in respect of matters specified under Kerala Service Rules, Financial code, or Treasury Code as well (SOM 110).

2.14 Whenever interpretation of a statute, statutory rule or judgment of a court becomes necessary, the opinion of the law Department shall be obtained. In addition, the draft notifications to be issued under various statutes, statement of facts and **other legal instruments** have to be got scrutinised by Law Department (SOM 112).

2.15 The note file contains the notes prepared by the officers who process the case and it shall run continuously as a single note with paragraphs numbered consecutively in the order in which they were written (SOM 75). "Case" consists of the current file, note file and any previous papers and books put up for reference (SOM 26). "Case" includes the papers under consideration and all previous papers and notes put up in connection therewith to enable the questions raised to be disposed of (2(i) G.S.I).

2.16 The signature at the end of a note of any officer of and above the grade of Under Secretary should be legible and should indicate the officer's designation (65(i) G.S.I).

2.17 Rule 11 of the Rules of Business and 71 of the Secretariat Instructions says that all orders or instruments made or executed

by or on behalf of the Government of the State shall be expressed to be made or executed in the name of the Governor. This Rule is in line with Article 299 of the Constitution of India which says that all contracts made in exercise of the executive power of the Union or State shall be expressed to be made by the President or by the Governor of the State, as the case may be, and all such contracts and all assurances of property made in the exercise of that power shall be executed on behalf of the President or the Governor by such persons and in such manner as he may direct or authorise.

2.18 Now we may examine whether the rules of procedure stated above have been followed in respect of the case on hand. Consequent to the appointment of the inquiry committee, the General Administration Department forwarded the basic materials which mainly included the File No. IT B1/16/2020/ITD (Computer No. 1480105) (the Note File and current file) as if this is the only file pertaining to the engagement of M/S. Sprinklr Inc. in the E&IT Department.

2.19 This file is a print out of the electronic file (Computer No. 1480105) started on 13.03.2020, 11.53 AM by Asst. IT (B1) Smt. Archana C.S. The note file contains 78 nos. of notes. Note No. 78 relates to Shri. Manesh Mohan SO, IT(B) and it bears the date 08.09.2020, 4.48 PM. After this note, a PDF note attachment has

been included as Note 43. This note contains 9 pages and 18 paragraphs. In the last line in page 9 it is seen written, "this may be added to the file already initiated in the Section in connection with Data Sharing for the Containment of COVID-19, so as to keep records comprehensive".

2.20 A signature and below it the date 11.05.2020 appear at the fag end of this page. Shri. M. Sivasankar, the then Principal Secretary, E&IT Department, has admitted, during his examination through video conference, that it is his signature. His name or designation is not available under this note. Shri. Vinod G. the then JS IT(B) now Additional Secretary has deposed before the committee, that the signature appearing below this PDF 'Note 43' belongs to Shri. M. Sivasankar.

2.21 Instruction 65 (i) of the Secretariat Instruction says that the signature at the end of a note of any officer of and above the grade of Under Secretary should be legible and should indicate the officer's designation. Though this note was prepared by Shri. M. Sivasankar, it does not have his official designation. It has been attached as 'Note PDF' on 18.05.2020 4.51 PM by Archana C.S. Asst. IT (B1).

2.22 Para 75 of the Kerala Secretariat Office Manual says that the note file contains the notes prepared by the officers who process the case and it shall run continuously as a single note with paragraphs numbered consecutively in the order in which they were written. Surprisingly this 'Note 43' does not contain any note, other than " 📎 note pdf " which is nothing but the notes prepared by Shri. M. Sivasankar, regarding engagement of M/S. Sprinklr Inc. for data analysis.

2.23 Smt. Archana C.S. the Assistant, E&IT Department while deposing before the committee has stated that no separate file relating to Sprinklr engagement has been raised in the department and the currents/correspondences regarding Sprinklr engagement were received in the section only on 18.05.2020. She would further state that on that day Shri. M. Sivasankar the then Principal Secretary gave her the "note pdf" along with certain records and directed to add the same in the file and accordingly she added "note pdf" as Note No. 43 in the Note File and added the records in the Current File No. IT.B1/16/2020/ITD under a single receipt. The currents handed over to the Assistant were numbered as Reference Nos. 1 to 34. Admittedly the reference numbers and dates there on were written by Shri. M. Sivasankar. The office section processed the same under a single receipt No.

4387144/2020/ITB as they were received in a bundle on 18.05.2020. Shri. Manesh Mohan, the Section Officer E&IT(B) and Shri. Vinod G, the then Joint Secretary E&IT Department also have deposed in tune with the facts stated by Smt. C.S. Archana. Further Shri. M. Sivasankar the then Principal Secretary E&IT Department has stated before the committee in the video conference that he had given the said note along with the reference Nos. 1 to 34 in the section only on 18.05.2020. So, till 18.05.2020 no file relating to Sprinklr engagement was initiated or processed in the E&IT Department as required by para 75 of the Kerala Secretariat Office Manual.

2.24 Whether the documents pertaining to the engagement of Sprinklr were executed in compliance of the Rules of Business deserves consideration. The Order Form (Reference 21), Master Service Agreement (USA) (Reference No. 23), SMMS Privacy Policy (Reference 24), Acceptable Use Policy (AUP) (Reference 25) and Mutual Non-Disclosure Agreement (Reference 33) are the documents relied on by Shri. M. Sivasankar to canvas for the position that the engagement of Sprinklr was in order. Reference No. 23 in the Current File is the agreement relied on by Shri. M. Sivasankar relating to engagement of M/S. Sprinklr for data analysis. Reference No. 23 is only a format of a Master Service

Agreement and as it was not seen to be an executed document, the E&IT Department was required to produce the executed original MSA before the Committee. The E&IT Department produced a similar format of the MSA and the Additional Secretary of that Department Shri. Vinod stated that this record alone was given by Shri. M. Sivasankar.

2.25 Shri. M. Sivasankar has stated during the video conference that the Master Service Agreement was not signed by the parties and according to him, since this is the Sprinklr format it is binding on Sprinklr. Shri. Jayasankar Prasad, M.D., KSITIL who had actively involved in this transaction along with Shri. M. Sivasankar also has stated that there was no need to sign this document as it is the Sprinklr format. He has admitted in the deposition given before Committee that all these formats MSA (USA), AUP, SLA, Order Form etc. are available in the site of Sprinklr and anybody can take printouts of the same. We are at a loss to understand the stand taken by Shri. M. Sivasankar and his associate as to how an agreement can bind the parties without execution as provided by law.

2.25.1 When we come to the basics of Master Service Agreement, it is clear that a Master Service Agreement is a contract between two parties in respect of a project of business relationship that offers

flexible system for completing a project over time when there will be decisions to be made along the way. The purpose of MSA is to set the bounds of the contractual relationship, establish a system for accomplishing the work that needs to be done and to provide an efficient way to keep the work on track and resolve any disputes which may arise during the course of the project. It is also the settled position that the MSA, by its nature should be customised to the needs of the parties and the projects they wish to pursue and there are no agreement formats that can take the place of a well drafted agreement tailored to the needs and capabilities of the parties themselves and the unique nature of their project. As the name implies, MSA is the master agreement that gives us the high level structure of the relationship between the parties. Following the MSA, there are usually queries of Statement of Works (SoWs) that outline the actual details of each phase of the project. No statement of works have been executed in relation to this engagement.

2.25.2 Therefore, essentially Master Service Agreement is the basic contract to be executed between the parties. Tagging an MSA format, that too, applicable to USA alone, along with other such records in the current file is of no use and consequence.

2.25.3　Another document relied on by Shri. M. Sivasankar is the Order Form (Reference 21). Even though some of the columns in the front page of the Order Form are seen filled up, and the Order Form was signed on 2.4.2020 by a person representing Sprinklr and by Shri. M. Sivasankar with nil date, the other columns are seen left blank. This also is found to be a Sprinklr format and it has not been executed for and on behalf of the Government of Kerala as required by the Rules of Business of the Government of Kerala.

2.25.4　As per the Master Service Agreement (USA) (Reference 23) Order Form means a written order executed by the parties which defines the respective order parameters and platform informations, such as, modules purchased, term and associated fees etc. This Order Form is found to be not appropriate to the needs of the Government as it is not accompanied by any Statement of Work (SoW). Moreover, it has been executed only on 02.04.2020 whereas the engagement of Sprinklr was well before that date. Data started uploading to the Sprinklr site at least by 25.03.2020 and at that point of time there was no document executed between M/S. Sprinklr Inc. and Government of Kerala.

2.25.5 Another document relied on by Shri. M. Sivasankar is the Service Level Agreement (Reference 22). This also is found to be not an executed agreement and so cannot be relied on for any purpose. Another document stated to have been executed is the Mutual Non-Disclosure Agreement (Reference 33). This is seen executed only on 14.04.2020. SMMS Privacy Policy (Reference 24) and Acceptable Use Policy (AUP) are simply Sprinklr formats available in their site and they are only helpful in getting an idea regarding their policy matters. Why these records have been handed over to the Section of the E&IT Department by the then Principal Secretary is not clear.

2.25.6 Thus, it could be seen that M/S. Sprinklr Inc. has been engaged for data analysis without executing necessary agreements or documents and in respect of the documents executed, the provisions of the Rules of Business and other laws have not been followed. After this matter became a controversy and after several cases were filed before the Hon'ble High Court, by 20.04.2020 this project was discontinued and the entire data was transferred to the State Data Centre. Even Shri. M. Sivasankar did not give any explanation during the virtual meeting as to why the MNDA was executed at such a long distance of time. Moreover the said agreement attached in this file does not appear to be appropriate

for a Government Department procuring cloud software services. Moreover it has not been executed as required by law.

2.26   The committee perused the file I.T.B1/16/2020 – ITD (Computer No. 1480105). The first word about M/S. Sprinklr Inc. in this file is Note No. 55 on 13.08.2020 at 5.04 PM by Shri. Manesh Mohan, S.O. IT(B) Department suggesting to terminate the agreement with Sprinklr.

2.27   All the papers in the custody of Shri. M. Sivasankar were added as currents to the existing file I.TB1/16/2020-ITD (Computer No. 1480105) so as to make it appear that the Sprinklr engagement file was already in process from early March, 2020. This type of file processing is against the established procedure contemplated in para 28 of the Kerala Secretariat Office Manual.

2.28   All these show clearly that there was no file processing in E&IT Department in relation to the engagement of Sprinklr for data analysis.

2.29   On a verification of the Master Service Agreement (USA) indicated as Reference No. 23 in the Current File and the evidence tendered by the officials of E&IT Department and the Institutional Heads working under E&IT Department, it is found that no contract or agreement was executed between M/S.

Sprinklr Inc. and Government of Kerala or E&IT Department regarding engagement of Sprinklr for data analysis. Shri. M. Sivasankar also has admitted that the Master Service Agreement was not executed.

2.30 Para 112 of the Kerala Secretariat Office Manual says that the statement of facts and other legal instruments have to be got scrutinised by Law Department. Rule 11 of the Rules of Business and Instruction 71 of the Secretariat Instructions say that all orders or instruments made or executed by or on behalf of the Government of the State shall be expressed to be made or executed in the name of the Governor. If the Law Department was consulted, the former Principal Secretary E&IT Department would have been in a position to ascertain how and in what manner a Master Service Agreement was to be executed.

2.31 Rule 10 (i) of the Rules of Business says that no department shall without previous consultation with Finance Department authorise any orders (other than orders pursuant to any general delegations made by Finance Department), which either immediately or by their repercussions will affect the finances of the State.

2.32 In the instant case Shri. M. Sivasankar has stated in his Note No. 43 that the service offered by M/S. Sprinklr was probono. The

version given by him to the committee in the video conference is that it is on the basis of the clause contained in the purchase order that he stated this service as probono. The above clause is as follows: "Customer is under no obligation to pay for the Sprinklr Services herein during the COVID-19 pandemic. Upon the conclusion of scoping and implementation, Sprinklr will provide customer with the pricing for the necessary services. At that time customer may, in its sole discretion, determine what amount, if any, it shall pay to Sprinklr for the Sprinklr Services."

2.33 The above clause clearly shows that even though the customer is under no obligation to pay for the services during the pandemic, upon conclusion of the scoping and implementation, the Sprinklr will provide the customer with the charges and at that time the customer may in its discretion pay the amount as decided by it. If both parties were of the view that the engagement of Sprnklr was free of cost, then a proper contract should have been executed incorporating a specific clause in this regard. As the engagement cannot be considered as cost free, the Finance Department should have been consulted.

2.34 Considering the totality of the circumstances and the facts borne out from the records and depositions, the Committee is of the view that no file has been processed in the E&IT Department in

Government in respect of engagement of M/S. Sprinklr Inc. for data analysis as required by the procedure laid down in the Rules of Business of Government of Kerala and the Kerala Secretariat Office Manual. Further, no agreement was executed between M/S. Sprinklr Inc. and Government of Kerala regarding Sprinklr engagement as require by law.

2.35 Since no file was processed and no agreement was executed in respect of engagement of M/S. Sprinklr Inc. for data analysis, we find that the relevant provisions in the Rules of Business of the Government of Kerala, the Secretariat Instructions and Secretariat Office Manual have not been followed in this case.

CHAPTER – III

What were the procedures to be followed apart from those that have been followed for the agreement/purchase order for obtaining services (Item No. IV in the term of reference)

3.1   After having discussed item No .1 in the terms of reference, we find it appropriate to consider this item taking into account its close connection with the first item in the terms of reference.

3.2   During the relevant period, that is, March and April 2020, Shri. M. Sivasankar was working as the Principal Secretary, E&IT Department. Shri. Vinod G. was working as Joint Secretary/ Additional Secretary E&IT Department, Smt. Archana C.S. was working as Assistant in the IT(B1) seat and Shri Manesh Mohan was working as Section Officer in the IT (B) Section. All these persons were examined and their depositions were recorded. All the heads of the institutions under the Administrative control of the E&IT Department also were examined and their depositions recorded.

3.3 As per the inputs received from the E&IT Department, the following Institutions viz.,

1. Kerala State IT Mission (KSITM)

2. Centre for Development of Imaging Technology (C-DIT)

3. Indian Institute of Information Technology and Management Kerala (IIITM – K)

4. Kerala Startup Mission (KSUM)

5. IT Parks (Technopark, Info park & Cyber park)

6. Kerala State IT Infrastructure Ltd. (KSITIL)

7. International Center for Free and Open Source Software (ICFOSS)

are functioning under the administrative control of the E&IT Department.

3.4 Shri Neelakantan, Deputy Director, IKM, Shri. Kannan, Special Secretary LSGD, Dr. Sabarish, Senior Principal Scientist, Science and Technology Department, Dr. Divya V.S., State Nodal Officer (Trainee), National Health Mission, Kerala and Shri. Biju S.B., Head of the Department of web services, C-DIT also were examined and their depositions recorded.

3.5 Sprinklr themselves declares in their FAQ about what they are and what they do. From this FAQ and other materials it is found that Sprinklr provides a cloud based Software application over the internet in a multi- tenant hosted environment. They say that

their SaaS model is fundamentally different from the other methods of software delivery. Sprinklr operates in a multi-tenant environment that runs the platform for all customers on a "single code line". The platform that is licensed to a customer is the platform readily available and already used by over thousands of customers of Sprinklr which is simply enabled to the new customer. From the SMMS Privacy Policy (Reference 24) and other records, it is found that Sprinklr basically provides a Social Media Management System (SMMS). The Sprinklr system is a tool that enables companies and organisations or Sprinklr customers to process and manage publically available infrastructure about their brand on the internet. It is also stated that Sprinklr requires each one of its customers to sign agreement with Sprinklr that align with Sprinklr Privacy Policies.

3.6 From the files, records and the depositions it is seen that during the early days of March 2020 the State witnessed huge migration of Keralites from other countries largely affected by COVID–19. Government of Kerala had the duty to control/check the spread of COVID -19 disease for which it was necessary for Government to put them in quarantine and monitor effectively. Collection of information of these people and their management were found to be crucial in the process of containment of

COVID-19. Apart from this, the data management issues dealt with by indigenous IT solutions deployed by different agencies were said to be not suitable as they were depending Google forms and excel sheets as the same were said to be providing cumbersome and erroneous information with inconsistencies and inaccuracies as deposed by Dr. Saji Gopinath, CEO, IIITMK & KSUM. As revealed from the deposition of Dr. Jayasankar Prasad Director, Kerala State IT Infrastructure Ltd. and Dr. Saji Gopinath and the notes of the technical committee, a strong need for a robust solution which should be fast and capable of managing multiple formats of large data volumes for addressing the COVID-19 Pandemic was considered necessary and the same was stated to have been discussed in the informal IT support team which consisted of Shri. M. Sivasankar as Chairman and the Heads of the Institutions under E&IT Department as members. Dr. Saji Gopinath informed before the committee that the IIITMK of which he was the CEO at that time had developed a food supply tracking and Management System for the use of the Civil Supplies Department to prevent shortage of food items during the period of COVID 19 pandemic. He further stated that IIITMK also analyzed large volume of PDS data to identify beneficiaries for providing welfare pension

support announced by the Government. Kerala start-up Mission of which also he was the CEO said to have identified start-ups to provide solutions like Direct Communications of Government to citizens to counter fake news. He also deposed that GOK Direct adopted by the Public Relations Department was later recognized globally as one of the unique COVID-19 management solutions. Effective telemedicine solutions like Quick Dr was adopted by IT Mission and Norka to provide telemedicine support to people on quarantine. Another solution, patient tracking solution called "Covid Tracker" was adopted by Kerala State Disaster Management Authority. As stated above, many organizations and individuals were said to be proposing solutions to address various issues relating to the COVID -19 pandemic. We were told that the Kerala Start-up Mission also started a portal for sourcing all such ideas and proposals for the analysis and support Implementation for the containment of COVID-19 pandemic. Other IT Institutions under the administrative control of E&IT Department also were seen to have tried their level best in this regard as deposed by them. While such solutions were being deployed, this committee was informed that there was an urgent need at that time for a more robust, better and "Comprehensive customer Relationship

Management" (CRM) solution with well built analytical capabilities at that time.

3.7   A detailed study has been made by the committee to ascertain as to when and in what manner the Sprinklr was engaged by E&IT Department for data analysis. As a matter of fact it is found that no agreement was executed in relation to the engagement of Sprinklr. Even the Purchase Order was signed by the representative of M/s Sprinklr Inc.and Sri M. Sivasankar only on 2nd April 2020 and its effective date is shown as 25.03.2020. Why this was given retrospective operation from 25.03.2020 is not clarified in that record. Admittedly Sprinklr service was being availed well before the date of the above purchase order. The circular dated 27.03.2020 (Reference 11) gives ample proof in this regard.

3.8   From File No. IT.B1/16/2020- ITD it is seen that formal offer to work with GOK was given to Shri. M. Sivasankar by the C.E.O, Sprinklr Shri Ragy Thomas through email dated 20.03.2020 at 6:16 pm (Reference 6). It is seen that this offer was in response to a proposal from Shri. M. Sivasankar which has been pasted below this mail. The said mail of Mr. M. Sivasankar has not been produced as a reference. When was that proposal given is not clear from the records. But in the pasted note it is stated that an

IT enabled database platform for increasing efficiency of fight against COVID-19, GoK was undertaking an all-encompassing effort to contain the spread of COVID-19 and to protect each and every person in the State from the possible hazard.

3.9   The records and evidences reveal that Shri. Arun Balachandran, CM's former IT Fellow had introduced M/S. Sprinklr Inc. to Shri. M. Sivasankar. This is spoken to by Shri. Saji Gopinath and Shri. Jayasankar Prasad during their examination before the Committee. Shri. Saji Gopinath has deposed that on March 19th 2020 CM's IT fellow Shri. Arun Balachandran has forwarded him the mail sent to IT Secretary and in that the Digital Contagion Management Solution's proposal was incorporated and on that night IT Secretary briefly discussed the matter over phone and to examine the proposal in detail, the IT Secretary has entrusted Dr. Jayasankar Prasad and an industry expert. Dr. Saji Gopinath has also stated that Arun Balachandran told him to explore the feasibility of integrating Sprinklr tools with GoK direct, and as per this he shared the details of the start up company which developed the solution GoK direct to Arun Balachandran. From the materials on record it is found that consequent to connecting M/S. Sprinklr with Mr. M. Sivasankar, Mr. M. Sivasankar had some discussions with Dr. Saji Gopinath, Dr. Jayasankar Prasad

and Sri. Arun Balachandran and then he forwarded a proposal which is the pasted note in the e-mail of Shri. Ragy Thomas dated 20.03.2020 and based on that proposal Ragy Thomas has mailed the offer and there upon Shri. M. Sivasankar engaged M/S. Sprinklr Inc. for the data analysis. Shri. M. Sivasankar has admitted in the virtual meeting that the URL: http://kerala.field-covid.sprinklr.com provided in the circular dated 27.03.2020 (Reference 11) was at his instance. Of course this URL was included by Dr. Chitra S., the then Director of KSITM and C-DIT. She was also then the Director of IKM. Shri. Kannan, Special Secretary, LSGD has deposed before the Committee that the name of this URL was given by IKM Director. The Principal Secretary LSGD, Smt. Sarada Muraleedharan, in a discussion over phone with the Chairman also has stated that the URL provided in the Circular of 27.03.2020 was given by Dr. Chitra S., who was then the head of the IKM. However, Shri. M. Sivasankar stated before the Committee during the video conference that this URL was given by him to Dr. Chitra for inclusion in the Circular dated 27.03.2020 issued by LSGD.

3.10 As per the Circular No. D.C.1/71/2020/LSGD dt 27.03.2020 (Reference 11) the URL http://Kerala-field-COVID.Sprinklr.com has

been provided to upload the data received as per the template appended to that circular.

It is relevant to point out that the template appended to this Circular (Reference 11) is having 24 columns which contain personal informations of persons under reverse quarantine (persons aged more than 60 years) and the direction in the Circular is to collect the details of such persons and to upload the same to the Sprinklr site shown under item 4 of the Circular. The above information definitely comes under the definition of sensitive personal data or information under Rule 3 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011. Rule 3(iii) states that sensitive personal data or information of a person means such personal information which consists of information relating to physical physiological and mental health condition and Rule 3 (i) states medical records and history. The information to be collected as per the template appended to the circular are regarding the physical and health condition of individuals with their identity.

3.11   From the above materials on record, it is found that sensitive personal information of the elderly citizens of Kerala were being uploaded to a web application provided by Sprinklr and it is

found that such is data is transmitted over internet to the web application using an unsecured method. No informed consent was being obtained from such persons. Before engaging a foreign agency for analysing such data, definitely the Hon'ble Chief Minister who was the Minister in charge of E&IT Department should have been duly informed and orders should have been obtained. In the case on hand there was not even a file regarding engagement of Sprinklr. It is also seen that there was a High Power Committee chaired by the Chief Secretary consisting of Department Heads. That Committee was also not consulted in respect of engagement of Sprinklr. It is also seen that the main activities regarding COVID-19 containment were done in the Health Department and LSGD also was involved in an all-encompassing effect in this regard. These departments also were not duly consulted before engaging Sprinklr for data analysis. The version of Shri. M. Sivasankar that these matters were discussed in the IT Support Team consisting of the Institutional Heads under him and the representatives of Health Department, LSGD, etc. were participating in such meetings cannot stand to legal scrutiny.

3.12   Dr. Chitra S, who was then the MD of KSITM and C-DIT which are under the administrative control of the E&IT Department of

which Shri. M. Sivasankar was the Principal Secretary, has deposed that there was no discussion regarding Sprinklr in such groups in her presence and she came to know of the same only from a telephone call made by Shri. M. Sivasankar after such engagement. Of course there were some discussions among Shri. M. Sivasankar, Dr. Jayasankar Prasad and Dr. Saji Gopinathan. But Shri. M. Sivasankar being the head of E&IT Department and others being officers under him, he alone can be held responsible for this engagement.

3.13 For procurement of a software service, the user Department is expected to make sure that necessary provisions are included in the MSA, SLA, NDA and other documents to ensure that required functionality is included in the proposed software, necessary security measures are incorporated at different levels and expected deliverables are supplied at expected period. It should also observe that its part in the bipartite contracts are met.

3.14 The CSP should be responsible to offer the user department with a software offering agreed functionality, mechanism implemented to meet the security expectations to ensure that unauthorised access or modification is not allowed to data while it is collected, transmitted over internet, stored on the cloud and

processed on the cloud, necessary trainings are provided to the Department's manpower regarding the use of functionality provided in the SaaS and deliverables are supplied at expected intervals.

3.15 Further the CSP also should ensure that the services offered under SaaS are available with automatic scale up and scale out to meet the user department performance requirements.

3.16 No such requirements (Statement of Work) have been incorporated in the Order Form. The order form and Master Services agreement (USA) are readymade formats for using B2B (Business to Business). But here B2C (Business to Citizens) formats were required. In B2C, company markets directly to an end user, where as in B2B, Company markets to a group. Government cannot be treated as a business entity and one among the group.

3.17 The Software as a Service has been obtained from M/S Sprinklr without respecting the procedure required to be followed to obtain SaaS for a Government department. The abstract procedure to be followed for procurement of SaaS is explained below:

The first two steps required in a process to procure a cloud service are deciding a cloud computing model and selecting a

cloud service. There are basically four types of cloud computing models namely Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud. Different cloud services available are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Selecting an appropriate cloud computing model is very crucial in ensuring security for the data involved. Private Cloud is offering higher security but, it is very costly. Hybrid Cloud is relatively cheaper when compared to private cloud which can also provide the required security when the system is properly designed. Among the various cloud services, SaaS is ideal when the Department has no competent in-house manpower to develop the required software applications.

3.18 There are some steps to be necessarily followed while procuring a SaaS from a CSP. First step is to decide the functionality to be provided by the SaaS. A Request for Proposal may be prepared to represent the required functionality. The next step is to decide security requirements to be met by the SaaS. Since, the CSP is having full control on the entire IT infrastructure including application software, ensuring security is the most important aspect when procuring a SaaS. The Department has to identify the sensitive data which need to be protected against unauthorised access. Legal Department should be consulted to

decide sensitive data involved. The Department should also decide various roles and access privileges for its manpower to access the functionality to be provided by the SaaS. Role based access privileges required by the department should be respected by the SaaS. Various deliverables expected from the CSP including functionality required in the SaaS and security requirements have to be clearly mentioned in the MSA or SLA whichever is appropriate.

3.19   MeitY has published guidelines regarding the procurement of a cloud service and regarding the SLA to be prepared while procuring a cloud service. It has also published a list of MietY empanelled CSPs.

3.20   The committee found from the documents supplied to it and from the discussions with the concerned parties examined that none of the above listed processes was completed by the Principal Secretary, E&ITD, GOK for engaging the M/s Sprinklr Inc. as a CSP for offering the SaaS.

3.21   Payment milestones for the Services has to be fixed. But in the instant case Order Form total has been put as TBD with asterisk and under the asterisk it is stated that the customer is under no obligation to pay for the Sprinklr services herein during the

COVID-19 pandemic upon the conclusion of scoping and implementation Sprinklr will provide customer with the pricing for the necessary Sprinklr Services. At that time customer may, in its sole discretion determine what amount, if any it shall pay to Sprinklr for the Sprinklr services.

As the workloads were unpredictable, this model might have resulted in high costs because of this TBD pricing (to be decided pricing).

3.22 There are multiple scenarios or engagement models on how government departments can procure cloud services. Therefore it is the duty of the department to choose the right scenario and accordingly specify the requirements in the Request For Proposal. (RFP).

3.23 Important considerations during procurement of Cloud Services are given below:

Government organisations should necessarily procure Cloud Services through Government e-marketplace (GeM) platform or through Bid Process/Reverse Auction (RA) functionality available on the GeM platform based on the total procurement value of the Cloud Services.

3.24 The user departments can refer to "Cloud Procurement Guidelines" for more details and assistance on how to procure Cloud Services through GeM.

3.25 Procurement of Cloud Services is a lengthy process and involves multiple phases with critical roles and responsibilities of all the Stakeholders in each phase. It is important that the right people do the right things at the right time.

3.26 Ideally, there are five phases involved when a Government Department plans to procure Cloud Services.

1. Planning

2. Design

3. Procurement and implementation

4. Operations and maintenance

5. Exit Management/Transition out.

Each phase is goal oriented and ends at a particular milestone.

3.27 In the planning phase Government departments need to draft a proper plan for procurement of Cloud Services.

Design phase is an early phase of a project where the key cloud requirements and Services are planned. Government departments may specify some additional requirements such as security, data backup, exit management, price discovery, auto

scaling limit, data retrieval period, data retention period, log access availability, logs retention period, backup requirements, data mirroring latency, data backup method, data backup frequency, back up retention time, back generations, maximum data Restoration, data portability format, data portability interface, data transfer rate, platform migration rate etc. in the RFP. In the procurement and implementation phase the departments may choose the lowest commercial quote (L1) or adopt a QCBS (Quality and Cost based Selection) as part of the commercials to procure the best fit solution for the department based on the project requirements. The departments based on the project requirements may include functional specifications in the RFP and evaluate the offered Cloud Solution against the compliances to the functional specification.

3.28 In addition to the compliance to the functional specifications, it may consider to have a Proof of Capability (POC) as part of the technical evaluation to demonstrate the key features such as auto scaling security controls, management and administration, logging and auditing capabilities of the offered cloud solutions. In such a scenario the departments may adopt a QCBS evaluation as part of the commercials to procure the best fit solution for the department.

3.29 User department will be responsible for the compliance with the Master Service Agreement, Order Forms and will be responsible for the accuracy, quality, and legality of their data, the means by which the department acquired this data and the use of data with the services.

3.30 The departments should necessarily review and validate the security configurations created by the CSP. Departments need to ensure that the CSPs facilities/services are certified to be compliant to the following standards:

1. ISO 27001

2. ISO 27017

3. ISO 27018

4. ISO 20000-1-

3.31 The department should monitor the operational activities to ascertain that the CSP has implemented the cloud features mentioned in the RFP.

3.32 As part of Exit Management/Transition out phase the department should separately indicate the requirements in the RFP.

3.33 Specific requirements for software as a service (SaaS)

The below mandatory requirements are applicable in addition to common technical control for services offered by CSP from software as a service, using Government community cloud or virtual private cloud or public cloud as cloud deployment models.

1. Cloud Services under SaaS model shall only be offered from Data Centres audited and qualified by STQC under the Cloud Services Empanelment Process.

2. CSPs shall be responsible for ensuring that all data functions and processing are performed within the boundaries of India.

3. CSPs shall be responsible to ensure that the services offered from SaaS provide a mechanism to authenticate and authorise users.

4. SaaS solution/services offered to user departments shall have in built functionality to integrate with existing authentication mechanism.

5. SaaS solution shall be able to segregate users on the basis of privileges granted to the users.

6. CSPs shall provision and implement role-based authentication when required and separation of identities shall be maintained in multi-tenant environment.

7. CSPs shall ensure that all the policies and procedures shall be established and maintained in support of data security to

include confidentiality, integrity and availability across various system interfaces and business functions to prevent any improper disclosures, alterations or destruction.

8.   CSPs shall ensure that any service offered from SaaS are monitored, controlled and administered using web based tool with visibility to the user Department.

9.   CSPs shall ensure that user Departments are provided with capability to generate custom report around several parameters such as users, time, data etc.

10.   CSPs shall be responsible to provide a mechanism to enable each user Departments' administrator to create, manage and delete user accounts for that tenant in the user account directory. CSPs shall ensure that services offered under SaaS are available with automatic scale up (adding more resources to handle demand) and scale out (adding more systems to handle demand) to meet user Department performance requirements.

11.   CSPs shall ensure that any service offered from the SaaS solution provider complies with P11 data security standards like ISO 27018.

12. CSPs shall ensure that services offered under SaaS are enabled with data loss prevention tools and capability to monitor data flow.

13. CSPs shall ensure that services offered under SaaS provide tools/capability for encryption of data-at-rest, data-in-processing and data-in-transit.

14. CSPs shall ensure that- services offered under SaaS support encryption algorithms like AES256 and higher.

3.34 In the instant case Cloud Services from a CSP called Sprinklr has been procured as direct purchase and not by using the Government e-Market place (GeM) which is a mandatory requirement to avoid corruption. Thus the established procedure being followed in Government departments in the Centre and in the States for procurement of Cloud Services are seen violated.

3.35 The project responsibility in respect of the critical security concerns are rest with the CSP, Sprinklr Inc.. No such provision has been incorporated in the Master Service Agreement.

3.36 The conventional IT projects have largely well-defined and accepted SLAs across the project domain. But SLAs are very critical to Cloud Services. Therefore it needs to be identified and

to be incorporated in the SLA. The same has not been done. Mere standard format has been used as SLA.

3.37 The mandatory requirements applicable to a CSP offering software as a service using Government community cloud or virtual private cloud or public cloud have not seen verified and confirmed while procuring Sprinklr SaaS for data analysis.

3.38 It is well understood that sensitive data collected should be masked before it is transmitted over internet. Secured methods have to be used by the softwares to transmit such data. It is evident from the URL specified in item 4 of the circular dated 27.03.2020 that unsecured protocol is used to transmit data.

3.39 The statement of work has not been specified in the order form whereby payment options were not seen considered. When the order form total stands TBD (to be decided later) the order form is not complete and unenforceable as there was no concluded contract as something of value has not seen exchanged.

3.40 It may be noted that direction for necessary API integration assistance to Sprinklr has been issued on 20.03.2020 at 10.16 PM through E-mail with specific instruction to make them live by tomorrow. It may be noted that all these arrangements have been done without issuing formal orders from Government in E&IT

Department and without the knowledge of the office in the E&ITD. Shri. M. Sivasankar is seen to have exercised the powers not by following the procedure contemplated in the Rules of Business and he has not addressed the data protection concerns. Even the link given in the L.S.G.D. circular dated 27.03.2020 does not satisfy the Security requirement. He had not seen ensured the Security of the endpoints that were used to access Cloud Services as part of Security Administration while procuring cloud service from a CSP.

3.41 Apart from the above it is found that the E&IT Department has not taken care of the other critical issues when dealing with Cloud contracts. The issues such as legal compliance, security and data management during exit in the cloud computing context were not seen addressed with reference to the structured data uploaded/given to M/S. Sprinklr for data analysis.

3.42 No Service Level Agreement has been executed. An SLA standardized with reference to the requirement of the Government was required to be executed as structured sensitive data were given for data analysis. Normally in the Service Level Agreement, a contractual agreement between a service provider and a consumer where the consumer's requirements are clearly specified and the service provider defines the level of service,

responsibilities, priorities, privacy and security and guarantees regarding availability, performance and other aspects of service. Since, critical sensitive personal data of citizens were uploaded to M/S. Sprinklr's SaaS platform the above aspects were to be necessarily addressed.

3.43 Being a Government department, the functional specifications stated in the offer of M/S. Sprinklr were not seen confirmed. As part of the technical evaluation the proof of capability of M/S. Sprinklr were not seen checked with reference to the requirements of Government.

3.44 When the structured sensitive personal data of citizens have been decided to be uploaded to M/S. Sprinklr's platform, the then Principal Secretary has not ensured before uploading the data that the services offered under SaaS are enabled with data loss prevention tools and its capability to monitor data flow.

3.45 As part of security, he has not ensured that the services offered under SaaS, support encryption algorithms like AES 256 and higher or comply with P11 data security standards like ISO 27018.

3.46 On pursuing the files and discussions with IT experts in the E&IT Department and other associated institutions, the Committee has

come to the conclusion that before engaging M/S. Sprinklr's SaaS platform, the security concerns have not been addressed.

3.47 Shri. M. Sivasankar and his close associate Dr. Jayasankar Prasad, M.D., KSITIL have not taken care to understand and address the risks and challenges associated with engaging M/S. Sprinklr for analysis of structured sensitive health data of citizen but seen given permission right away.

3.48 The question of increased risks of compromise of confidential information and inappropriate/ unauthorised access to personal information were not seen considered before handing over/uploading personal data in the structured format to M/S. Sprinklr's SaaS.

3.49 The standards around integration, data security, portability, operational aspects, contract management etc. prescribed for engaging a Cloud Service Provider by MeitY were not taken care of by the Principal Secretary before deciding to use Sprinklr SaaS cloud.

3.50 The G1 Cloud is the Government of India's Cloud Computing Environment that is used by Government Departments and agencies at the Centre and States. In other words, it enables the

Government Departments in Centre and States to leverage cloud computing for effective delivery of services.

3.51 The Government Community Cloud serves Central and State Government organisations delivering dynamic IT governance. The Government Community Cloud secures the confidential data of the Government by allowing only Government entities to access the cloud infrastructure and by ensuring that the data is stored within the Indian geographical borders.

3.52 It is seen that N.I.C has established the Centre of Excellence for Data Analysis "CEDA" to assist government organisations to derive insights from their data. They claim that CEDA provides world class Data Analytics Services to Government in an efficient and secure manner through its repository of world class tools and technologies. But it is not clear from the file and the depositions of IT experts that the then Principal Secretary has not explored this possibility before resorting to Sprinklr for data analysis.

3.53 In the order form it has been stated that customer is under no obligation to pay for the Sprinklr Services herein during the COVID-19 pandemic. Upon the conclusion of scoping and implementation Sprinklr will provide customer with pricing for necessary Sprinklr Services. (Page 129). Therefore the decision

to engage M/S. Sprinklr by M. Sivasankar was not for a short period.

3.54 As it is stated by Sprinklr, Sprinklr's SaaS model is fundamentally different from other models of software delivery. The platform that Sprinklr license to Government is the one readily available and already used by over thousand customers of Sprinklr. Existing software licensing models may not facilitate cloud deployment especially from the point of cloud service delivery. To facilitate Government departments in deployment of Cloud Services a comprehensive framework has been developed by MeitY (GoI) on the usage of various licensing models. The framework to be selected must be flexible to take into account emerging technologies and business models to leverage the same in the best interest of Government. The same was not considered when the order form was issued by the former Principal Secretary to M/S. Sprinklr Inc.

3.55 Government Departments are required to ensure quality certification process while adopting cloud that the solutions being given should meet minimum quality bench marks. To ensure a quality product it would be required that the solution should qualify functional testing and performance testing through STQC. The same was not seen done before engaging M/S. Sprinklr. Apart

from following the procedure for file processing as provided under the Rules of Business/ Secretariat office manual/ Secretariat instructions for giving formal sanction for the engagement of a Cloud Service Provider/ procurement of a Cloud Software Services as described in Chapter II of this report, the other responsibilities of the Government Department to be complied with especially technical aspects before procuring the Cloud Software Services, and the non-fulfilment of the same by the E&IT Department in the process of procuring SaaS from M/S. Sprinklr has been discussed in detail in the pre paras to address the question in the 4th item of the terms of reference that what were the procedures to be followed apart from those that have been followed for the agreement/purchase order for obtaining services.

CHAPTER – IV

What are and what could have been the measures taken to ensure data security at various periods (Item III of the Terms of References)

4.   Data security is the practice of protecting digital information from unauthorised access, out of computers networks, websites and databases. The process also provides a mechanism for protecting data from loss. There are several types of data security measures, such as data backup, firewall, data encryption, authentication, antivirus software, digital signature etc.

4.1   As per our study/inquiry on the area of security parameters to be considered by the E&IT department in procuring the SaaS Sprinklr Cloud Software, no guidelines issued in this regard have been followed. On account of non-execution of MSA, SLA and NDA it is seen that no measures are seen to have been taken to ensure data security in the engagement of Sprinklr by E&IT Department.

4.1.1 For the purpose of ensuring data security, the user department needs to ensure that the security guidelines such as those defined by STQC are to be met by the CSP.

4.1.2 The Government Departments will have to configure their IT environments in a secure and controlled manner for their security purposes. Government departments will have to review and validate security configurations created by CSP. Departments need to ensure that the CSP's facilities/services are certified to be compliant to various ISO standards.

4.1.3 The user department shall ensure that the provisioning, installation, configuration, management, monitoring of security services have been done by the CSP as per the requirements of the user department.

4.1.4 The user department shall ensure that the CSP has the capability to identify security configuration gaps. The user department has also to ensure that there is provision to manage and deploy High Security Module (HSM) as per their requirements.

4.2 *While developing an application architecture for the cloud, following steps need to be considered for the user departments:*

4.2.0 Measures to be taken to protect sensitive data from unauthorised access is an important step since, use of cloud may involve transmission/ processing / storage of sensitive data outside the premises of the Government Department. An appropriate cloud computing model (Public / Private / Hybrid /

Community) needs to be selected. It is advisable to opt for a hybrid model where sensitive data is stored and processed in a private cloud maintained in the premises of the Government Department. Also, adequate mechanisms should be provided to ensure that data on public cloud is secured.

4.2.1   There is a fundamental concept of Service Oriented Computing. It ensures that application's components are treated individually, and dependencies are reduced. It further ensures that addition, removal, failure or update of one component has a minimum impact on other components. Thus, it is always recommended to develop components separately and define their integration/interaction mechanism in a separate component.

4.2.2   Each service operation should ideally perform single transaction to simplify error detection, error recovery, and simplify the overall design. Each service operation should map to a single business function, although if a single operation can provide multiple functions without adding design complexity or increasing message sizes, it can generally reduce implementation and usage costs.

4.2.3   Private and public clouds are complex distributed systems that work best with application architectures that break out processing and data into separate components. By duplication,

the data can be stored and processed on any public or private cloud instances. In such cases latency may occur, so it is recommended to use caching systems. These provide additional database performance by locally storing commonly accessed data, thereby reducing all database read requests back to the physical database.

4.2.4   Application components that communicate with each other continuously may lower the performance of the overall application. In order to improve the performance combining the communications into a single stream of data, rather than constantly sending messages is the best practice.

4.2.5   A test case should be built that represents how an application behaves under an increased load. While the traffic increases, the number of web server and associated database instances may have to be increased to handle any additional load. This can help to understand the process to scale the application by automatically increasing resource on the instances for load balancing. In some cases, Cloud service providers offer auto-scaling capabilities, where provisioning occurs automatically. In this manner, it becomes easier to understand the application's workload profile and to define the path to scale the application.

4.2.6   Developing solution architecture that focus on mature Identity and Access Management capabilities can reduce security costs for Government Departments.

4.3   ***Below are the key factors that a Government Department may consider when carrying out Capacity Sizing for Storage.***

4.3.1   Storage must be configured with enough disk drives to meet the IOPS and latency needs of the applications.

4.3.2   When carrying out sizing for storage required on Cloud, the Government Department must consider the type of data that is proposed to be stored on the disk.

4.3.3   The Government Department must identify and segregate the type of work load in accordance with Production / Development / Test Environment and performance needs.

4.3.4   The Government Department may opt for SSD / Flash disks, SAS, SATA / NL-SAS as per the type of data that is to be stored and accessed. SSD /Flash drives shall offer highest performance in terms of high IOPS requirement.

4.3.5   The Government Department shall define the IOPS requirements and storage capacity specific to application and associated databases performance needs.

4.3.6   The Government Department may opt for 20% buffer when procuring Storage and Cloud to meet increasing demand.

4.3.7   Storage infrastructure should be organized such that it is efficient enough to upgrade and add capacity to take care of any additional performance requirements.

4.3.8   Flash drives may be considered and sized for high transaction databases, roll-back segments and frequently accessed tables, frequently accessed web content, applications with high random read requirements and business-critical applications impacted by low cache read hit rates.

4.4   ***Network and Security capacity planning involves:***

4.4.1   Structuring the network from the perspective of Utilization, the amount of material or items passing through system or process, Operations, availability and other network constraints.

4.4.2   Sizing the Security components from the perspective of Throughput, User Count, Bandwidth, Transactions per second and other security constraints.

4.5   Below are the key factors that a Government Department may consider when carrying out Capacity Sizing for its network and security infrastructure:-

4.5.1   For assessment of network components required to be procured on Cloud, the key task is to understand and analyse the current network traffic volumes.

4.5.2   It is essential for the Government Departments to understand the current network utilization patterns to cater to the increase in traffic and bandwidth requirement for procuring network services accordingly.

4.5.3   If the Government Department currently has multiple connectivity options such as, MPLS, VPN, Point to Point, Internet Leased Line in its infrastructure setup, then the Government Department should adopt adequate measures in order to support the same connectivity options when migrating to Cloud Service Provider platform.

4.5.4   Assessment of Government Department current security posture, including but not limited to Firewalls, IPS, IDS, HIPS, Antivirus, SIEM, End Point Protection, DLP, DDoS protection and mitigation.

4.5.5   Government Department must ensure equivalence to current and future security requirements while carrying out capacity sizing to migrate to Cloud.

4.5.6   This analysis shall help the Government Department to understand the amount of N/w & security resources needed to cater to the future requirements.

4.6   ***It is important for applications to adhere to quality certification processes to ensure that solutions being given for replications***

to other stakeholders, meets minimum quality benchmarks. To ensure a quality product it would be required that the solution:

4.6.1   Should qualify defined functional testing through STQC.

4.6.2   Should qualify defined performance testing through STQC.

4.6.3   Should qualify standard security testing criteria.

4.6.4   Should have well documented development and testing process artifacts.

4.7   As part of addressing data security measures it is helpful to know the order of the Hon'ble High Court dt. 24.04.2020 and various other decisions of High Courts and other forums and the measures under taken for the protection of sensitive personal data.

Shri. Balu Gopalakrishnan (WP (C) No. 9498 of 2020) (WP (C) Temp No. 84 of 2020) Shri. Michael Varghese (WP (C) No. 9530 of 2020) (WP (C) Temp No. 129 of 2020) Shri. K. Surendran (WP (C) No. 9530 of 2020) (WP (C) No. 132 of 2020) Shri. Ramesh Chennithala (WP (C) No. 9532 of 2020) (WP (C) No. 148 of 2020) Shri. Binosh Alex Bruce (WP (C) No. 9532 of 2020) (WP (C) No. 163 of 2020) filed writ petitions before the Hon'ble High Court and the Hon'ble High Court on 24.4.2020 has issued an order and among other things directed the Government of Kerala and its concerned departments to anonymise data that

have been collected and collated from the citizens of the State with respect to COVID-19 epidemic, as also with respect to all data to be collected in future and to allow Sprinklr to have further access to any such data only after the process of anonymisation is completed.

Apart from the above, Shri. N.S. Gopakumar, Jothikumar Chamakkala, Abdul Jabbarudeen. M and advocate Krsihna Prasad. N have filed public interest litigations and all the above cases are still pending before the Hon'ble High Court.

4.8 As stated above, the Kerala High Court in the case in Balu Gopalakrishnan V. State of Kerala (WP(C) 9498/2020) passed interim order on 24 April, 2020 on the export of COVID-19 related data by the Government of Kerala to a US based entity, Sprinklr, for data analysis. This order sets an important benchmark for all public-private partnerships in the post COVID-19 era in the field of data protection and emphasises the accountability of the State in handling data of its citizens.

4.9 The Odisha High Court in the case of Subranshu Rout@Gugul V. State of Odisha BLAPL No. 4592 of 2020 in its order dated 23rd November 2020 highlighted the importance of the right to be forgotten of an individual and how it remains unaddressed in legislation. The case involved objectionable content regarding a

women that was posted on line. While the victim had not made any arguments with regard to the permanent removal of her data, the court encouraged the victim to seek appropriate orders for the protection of her fundamental rights to privacy even in the absence of an explicit right to be forgotten.

4.10   In the global data protection law, the Court of Justice of the European Union (CJEU) in a case popularly known as Schrems 11 case C 311/18 Data Protection Commissioner V. Facebook Ireland Limited and Maximillian Schrems, invalidated the EU-US privacy shield claimed by Sprinklr in their document shown as current page number 167 of File No. IT-B1/16/2020-ITD (Computer No. 1480105) and read down the inviobility of the Standard Contractual Clauses (SCC). The privacy shield is an adequacy decision issued by the European Commission (E.C.) regulating data transfers between the United States of America (U.S) and any Member States of the European Union (E.U) or the European Economic Area (EEA). The CJEU invalidated the E.C. decision approving the privacy shield observing that due to the operation of Surveillance Laws in the U.S. the privacy shield does not provide adequate protection rights of an individual that is similar to the GDPR. It also ruled that the SCCs by themselves do not provide adequate protection of an individual's data

protection rights and additional due diligence of the transferee's country's laws has to be made to be a legitimate cross-border transfer of data under the GDPR.

4.11 Several measures have been taken by the Central Government in tune with GDPR. PDP Bill was proposed in 2019 to bring about a comprehensive overhaul to India's current data protection regime, which is currently governed by IT Act, 2000 and the rules there under. The current draft of the PDP Bill prescribes compliance requirements for all forms of personal data, broadens the rights given to individuals, introduces a central data protection regulator, as well as institutes data localisation requirements for certain forms of sensitive data.

4.12 MeitY, Government of India have constituted a committee "NPD Committee" to explore the governance of non-personal data. This committee defined non-personal data as data which is not personal data as per the personal data protection Bill, 2019 or data without any personally identifiable information.

4.13 National Digital Health Mission (NDHM) was announced by MOHFW and in late 2019 recommending the creation of a National Digital Ecosystem which allows for interoperability of digital health systems at the patient, hospital and ancillary health care provider level. On 20.12.2020 MOHFW approved a Health

Data Management Policy largely based on the PDP Bill to govern data in the Ecosystem.

4.14   NITI Aayog in August 2020 has released a draft framework on Data Empowerment and Protection Architecture (DEPA) in consultation with a few industry regulators, banks, and fintech players. Though DEPA and NITI Aayog aims to institute a mechanism to secure consent based data sharing in the fintech sector which they believe will be a historic step towards empowering individual with control over their personal data.

4.15   There is no express legislation in India dealing with data protection, the Personal Data Protection Bill which was introduced in Parliament in 2006 is yet to become a statute. The Bill aims to proceed on the general framework of the European Union Data Privacy Directive, 1998 which was implemented from 24.10.1998. The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

4.16   Section 72 of IT Act is limited to information being obtained by virtue of a power granted under the IT Act Section 72A on the

other hand extends to disclosure of personal information of a person without consent while providing services under a lawful contract and not merely disclosure of information obtained by virtue of powers granted under the IT Act.

4.17   Clause 32 Chapter VI of the DNA Technology (Use and Application) Regulation Bill, 2019, deals with Security and Confidentiality of information.

4.18   There are currently sixteen different Facial Recognition Tracking (FRT) Systems in active utilisation of various Central and State Governments across India for Surveillance, Security or authentication of identity. Another seventeen are in the process of being installed by different government departments.

4.19   While the FRT system has seen rapid deployment by multiple government departments in recent times, there are no specific laws or guidelines to regulate the use of this potentially invasive technology.

4.20   Legal experts say that this poses huge threat to the fundamental rights to privacy and freedom of speech and expression because it does not satisfy the Supreme Court's land mark privacy judgment in the Justice K.S. Puttaswamy V. Union of India.

4.21   There are organisations like Free Software Movement of India, Democratic Alliance for Knowledge Freedom, Software Freedom

Law Centre, Internet Freedom Foundation and other coalitions who are asking for fixing procedures and operational guidelines in the use of these technologies to protect and guard the data privacy of individuals.

4.22 The Hon'ble Supreme Court in Puttaswamy case ruled that privacy is a fundamental right even in public places.

4.23 The Personal Data Protection Bill again was introduced in the Parliament in December, 2019. The PDB Bill is based on the Parliamentary committees proposal with a number of notable differences.

CHAPTER –V

Whether lapses, which cannot be justified in the extraordinary circumstances prevailing while entering into the agreement / purchase, order, have occurred? (Item No. IV in the terms of reference)

The following are identified as the main lapses that have occurred while engaging Sprinklr for data analysis.

5.1   No file has been processed in the E&IT Department in Government to engage M/S. Sprinklr for data analysis as required by the procedure laid down in the Rules of Business of Government of Kerala and Secretariat Office Manual.

5.2   The file seen to have been processed relating to enagement of Sprinklr was on the currents (Reference 1 to 34) handed over by Shri. M. Sivasankar to Smt. Archana, Section Assistant of E&IT Department and attached to the existing current file No. IT B1/16/ITD on 18.05.2020 and attached the "note pdf" as Note No. 43 in the note file. This method adopted by Shri. M. Sivasankar seems to be to make it appear that the file in relation to Sprinklr

engagement was already under process. This was totally against the procedure laid down in Chapter VII of the Secretarial Office Manual.

5.3 Government of India, MeitY has prescribed guidelines for the procurement of Cloud Services by a Government Department from a Cloud Service Provider. Procurement of Cloud Services shall be made either through the Gem Market Place or through the Bid Process/Reverse Auction (RA) functionality available on the GeM platform. That has not been done in this case.

5.4 Since E&IT Department is the purchaser department for procuring the Cloud Services for data analysis, the terms and conditions of the MSA should at all-time be construed in accordance with the provisions of IT Act, 2000 and the Rules and Regulations issued thereunder besides the provisions of privacy laws and other applicable laws of India. The MSA itself has not been executed in respect of M/S. Sprinklr engagement. Further the MSA format available in the file is not the appropriate format. Moreover, provision should have been incorporated in the MSA to the effect that all legal disputes were subject to the exclusive jurisdiction of the courts, where the purchaser was located. The jurisdiction in the Master Service Agreement (USA) format happened to be the Federal Courts located in New York City for the reason that this

format is for the use of Sprinklr engagement in USA. They have such formats for all countries where they have activity and and such formats with the name of such countries are available in their site. So even this MSA (USA) format was not appropriate for their engagement in Kerala.

5.5   The SLA had to be prepared incorporating the key service level objectives identified indicating the measurement methodology to be adapted for measuring the services by defining the target levels and penalties to be levied in case of non-performance. But here only a standard format is seen kept in the file as reference (22) which is not in accordance with the guidelines issued by MeitY, Government of India to be used by departments for Service Level Agreements for procuring Cloud Services. Further the said SLA has not been executed between M/S. Sprinklr Inc. and Government of Kerala. This SLA format is of no significance in the eye of law.

5.6   In the order form it has been stated that the customer is under no obligation to pay for the Sprinklr Services herein during the COVID-19 pandemic. Upon the conclusion of scoping and implementation, Sprinklr will provide the customer with the pricing for the necessary services, and at that time the customer may in its sole discretion determine what amount it shall pay to Sprinklr.

The E&IT Department did not consult Finance Department on the premises that Sprinklr service was probono. But this was not correct. Since the repercussions after COVID-19 pandemic on the Sprinklr engagement ought to have affected the finances of the State, the Finance Department should have necessarily been consulted as provided under Rule 10 (i) of the Rules of Business. But the same was not done.

5.7 The MSA, SLA, Order Form and MNDA are not the appropriate formats to be used for a government department while procuring Cloud Software Services. As per para 112 of the Kerala Secretariat Manual it has been stated that all legal instruments have to be got scrutinised by Law Department. Since these instruments were not scrutinised by Law Department its appropriateness for the usage of E&IT Department could not be confirmed by E&IT Department.

5.8 Rule 11 of the Rules of Business and Instruction 71 of the Secretariat instructions say that all orders or instruments made or executed by or on behalf of the Government of the State shall be expressed to be made or executed in the name of the Governor. Rule 11 of the Rules of Business has been incorporated in the Business Rules in Compliance of the provisions contained in Article 299 (1) of the Constitution of India which are mandatory in

character and any contravention there of nullifies the contract and makes the agreement void. In the case on hand the Order Form and MNDA have been executed in the name of former Principal Secretary and have not been expressed to be made or executed in the name of the Governor.

5.9 The then Principal Secretary did not even ensure the basic security measures to be adopted while engaging Sprinklr. No agreements or documents have been executed as required by law for ensuring data security. Moreover, while providing the URL in the LSGD circular dated 27.03.2020 for uploading data, Shri. M. Sivasankar failed to ensure the security standards to be followed for transmitting sensitive data over internet.

5.10 Government Departments including Government Secretariat was under lock down during March, April 2020. According to Shri M. Sivasankar there was urgent need for a robost, better and Comprehensive Customer Relationship Management Solution with well-built analytical capabilities was reported to be necessary during the time of COVID-19 pandemic and so he proceeded to engage Sprinklr which is a Cloud Service Provider.

5.11 Vetting of the documents to be executed and examining the feasibility of the project were done as an in house mechanism

consisting of a technical team formed by the former I.T. Secretary for the sole purpose and not in accordance with the established Rules and Procedures as deposed by the institutional heads working under the Administrative Control of E&I.T. Department.

5.12 The Log Analysis Audit and Assessment Report of Sprinklr Application platform conducted by a CERT-In empaneled audit agency in their report dated 17.05.2020 has categorically stated that during their assessment they found that there was no unauthorised access been identified and there was no sign of data leakage or breach happened on the Sprinklr application during the logged period (April 3rd 2020 to April 19th 2020) which clearly ensured the security of the endpoints that were used to access Cloud Services.

5.13 We have already found in the earlier Chapters that the whole responsibility for the engagement of Sprinklr was with Shri. M. Sivasankar, the then Principal Secretary E&IT Department. He himself is found to have shouldered that responsibility publically. No doubt the lapses occurred in engaging Sprinklr for data analysis mentioned in the pre-paras are serious. However, despite such lapses, on a totality of all facts and materials on record and taking note of the extra-ordinary circumstances prevailing at that point of time, the Committee is of the view that

no evil design, malice or bad faith can be attributed upon Shri. M. Sivasankar for his lapses in engaging Sprinklr for data analysis. He appears to have pursued the SaaS simply as a product and proceeded to purchase the same on the premises that it was given probono and in his capacity as the Head of the E&IT Department he was empowered to purchase it by following the provisions of the Store Purchase Manual. The whole activities with Sprinklr continued only for less than a month. No payment was made to Sprinklr. The Sprinklr activities continued only for less than a month and by 20.04.2020, the entire data has already been transferred to the State Data Centre managed by C-DIT and instructions were also given to destroy data if any remained with Sprinklr forthwith. Accordingly Sprinklr reported compliance with the same. There is no evidence, as of now, to vindicate that the interest of the State was adversely affected due to the engagement of Sprinklr.

5.14 Considering all aspects enumerated in the pre paras, the Government may take an appropriate decision regarding the future course of action.

CHAPTER – VI

Analysis of the report submitted by the Committee headed by Shri. M. Madhavan Nambiar (Vth item of the terms of reference)

6.1 The Expert Committee constituted under the Chairmanship of Shri. M. Madhavan Nambiar IAS (Retd.) to inquire into the Sprinklr issues were authorised to examine the following:

6.1.1 Whether the privacy of personal and sensitive data of individuals has been adequately protected under the agreements entered into with Sprinklr.

6.1.2 Whether adequate procedures have been followed while finalizing the arrangements with Sprinklr Inc.?

6.1.3. Whether deviations, if any are fair, justified and reasonable considering the extra ordinary and critical situation the State was facing at the relevant period?

6.1.4 Any other suggestions for future guidance?

6.2 Of course this Committee feels considerable delicacy in analysing the report of the earlier committee as it was prepared by such eminent persons. However in view of the specific item V in the terms of reference, this committee is constrained to specify few aspects of the above report.

6.3 In para 3 of the executive summary it has been stated that the IT Department entered into multiple agreements with U.S. based Sprinklr Inc. as it was felt that the State needed multi-dimensional data-analytics solutions related to COVID-19 cases. But in fact apart from signing of the Order Form, no agreements such as Master Service Agreement and Service Level Agreement etc. were executed between GoK and with M/S. Sprinklr Inc.

6.4 In the 4th para of the executive summary it has been stated "the data will be initially hosted in the computers of Sprinklr Inc. hired by them at AWS, Mumbai and the entire data and applications would then be transferred to computers of C-DIT as soon as the same was ready. The data was however, to be managed by Sprinklr Inc. at all times." But in fact no agreement or understanding to this effect was made with M/S. Sprinklr and GoK. Then how this statement found a place in the Executive Summary is not clear.

6.5   In the 7th para of the Executive Summary it is seen stated that it would be very difficult to enforce penalty for any violation of the agreement clauses (including breach of privacy, confidentiality and security of data) as the jurisdiction of the agreements was at Courts of New York, USA. Factually and legally the MSA being an unexecuted document the above clause was of no significance. Shri. M. Madhavan Nambiar Committee is found to have proceeded on the mistaken premises that such agreements were executed between Sprinklr and GoK.

6.6   Shri. Madhavan Nambiar Committee formulates their report on the basis of the understanding that the SaaS product of M/S. Sprinklr was offered on a brobono basis. But it was not so as explained by M/S. Sprinklr in the order form itself.

6.7   Shri. M. Madhavan Nambiar Committee has stated in pages 11 and 12 under the heading 'Agreement with Sprinklr Inc.' that Mr. M. Sivasankar had executed an agreement with M/S. Sprinklr Inc. on 12th April 2020. But this statements does not appear to be correct. No agreement was executed on 12.04.2020 and it was only a letter sent by the General Counsel, Shri. Danhaley to Shri. M. Sivasankar by e-mail.

CHAPTER – VII

Suggest Guidelines to be followed in future (item VII of the terms of references)

1. As cloud computing is becoming an increasingly attractive model for delivery of infrastructure and other services primarily due to its essential characteristics of on-demand self services and elasticity etc., several Government departments are showing interest in procuring cloud services. While doing so, as far as possible, Government departments are advised to procure Cloud services through the GeM platform only. When the requirement of a particular department is met by a CSP whose services are yet to be listed in the Government e-market place (GeM) that Department may procure their services only after getting them successfully empaneled with MeitY.

2. There are multiple divisions under the E&IT Dept that evolved over time and some of them are unique to Kerala and some of them which the other states later followed. Given the decentralised development model adopted in Kerala it will be important to have distributed Data Centres across kerala that would manage the Cloud infrastructure. Government of Kerala may setup its own

Cloud infrastructure for all purposes, that includes e-governance and ensure all departments use it for their requirements.

3. The E&IT Department may recruit the minimum required regular employees with necessary qualifications to form a Technical Expert Team (TET) in the department to advise the Government in developing/procuring, deploying and maintaining software applications.

4. Ensure that application logs and database logs are kept until these are analysed to verify that unauthorised accesses were not happened to the application softwares and databases on the system.

5. Ensure that a role based fine grained access control mechanism is planned, implemented and maintained.

6. Follow the guidelines issued by MeitY regarding the enablement of Government Departments for adoption of cloud.

7 Follow the guidelines issued by MeitY for procurement of cloud services.

8 Whenever possible, take cloud service from a CSP included in the MeitY empanelled list of CSPs.

9 Functionality of the required application software should be finalised before selecting a SaaS. TET shall be entrusted to prepare software requirement specification.

10 Required provisions for ensuring security, functionality required in case of SaaS and other such deliverables should be made a part of the Service Level Agreement or Master Service Agreement whichever is appropriate.

11 Follow the guidelines issued by MeitY regarding Service Level Agreement for procuring cloud services.

12 Specific guidelines for the engagement of Cloud Services in Government Departments are specified in Appendix V.