THE HIGH COURT OF MEGHALAYA
SHILLONG

NOTIFICATION

Dated Shillong, the 29th August, 2025

No. HCM.II/60/2023/Estt/24 : In compliance with Order dated 11.08.2023 passed by the Hon'ble Supreme Court of India in Writ Petition (Crl.) No. 99/2015 – *Pradyuman Bisht vs Union of India & Ors.*, the High Court of Meghalaya is pleased to notify the **Guidelines on Data and Privacy** for the High Court of Meghalaya and District Judiciary in the State of Meghalaya.

All concerned are directed to ensure strict compliance with the Guidelines with immediate effect.

By Order

/

REGISTRAR GENERAL

Memo No. HCM.II/60/2023/Estt/24-A **Dated Shillong, the 29th August, 2025**

Copy to:-

1. The Registrar cum Principal Private Secretary to the Hon'ble the Chief Justice, High Court of Meghalaya for favour of his Lordship's kind information.
2. The Private Secretary to Hon'ble Mr. Justice H.S. Thangkhiew, Judge, High Court of Meghalaya for favour of his Lordship's kind information.
3. The Private Secretary to Hon'ble Mr. Justice W. Diengdoh, Judge, High Court of Meghalaya for favour of his Lordship's kind information.
4. The Private Secretary to Hon'ble Mr. Justice B. Bhattacharjee, Addl. Judge, High Court of Meghalaya, for favour of his Lordship's kind information.
5. All District & Sessions Judges in Meghalaya for information and necessary compliance.
6. Registrar (Judicial Services) –cum- Central Project Coordination, High Court of Meghalaya for favour of kind information.
7. Joint Registrar –cum- OSD to Hon'ble the Chief Justice, High Court of Meghalaya for favour of kind information.
8. System Analyst, High Court of Meghalaya, Shillong for uploading the same on the official website.
9. Office Copy.

2951
29/8/25

REGISTRAR GENERAL

-23

REPORT OF THE COMMITTEE ON DATA AND PRIVACY FOR THE HIGH COURT OF MEGHALAYA AND THE DISTRICT COURTS

Right to privacy and data protection: The right to privacy includes the right to be free from unwarranted intrusion into one's personal life, including the right to privacy of one's thoughts, feelings, and emotions. Thus, it extends to include bodily integrity, personal autonomy, informational self-determination, protection from surveillance, dignity, confidentiality, compelled speech and freedom to dissent or move or think. The right to privacy also includes the right to be free from unwarranted collection, use, and disclosure of personal information. Data protection is important not only for litigants but also for the personnel working in the institution itself. It is important to protect the privacy of data so that it can be used in a responsible way. A nine-judge Constitution Bench headed by Hon'ble the Chief Justice, J.S. Khehar on 24th August, 2017 gave a landmark decision on Right to Privacy. Hon'ble the Supreme Court ruled that Right to Privacy is "intrinsic to life and personal liberty" and is inherently protected under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution. Since the protection of data falls under the right to livelihood, then it cannot be violated and taken away except in accordance with due procedure of law. The existing legal framework also recognizes one's right on his/her private property. Article 12 of the Universal Declaration of Human Rights, 1948 and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), 1966 legally protect persons against "arbitrary interference" with one's privacy, family, home, correspondence, honour and reputation.

1. **Why right to privacy and data protection is necessary**: First and foremost, privacy is necessary for our personal safety. If our personal information is publicly available, there is every possibility that it can be used to harm us and / or control us against our will. Secondly, privacy is necessary for our personal dignity. If unwanted personal information is publicly available, it can be used to humiliate and shame a person. Thirdly, privacy is necessary for inter-personal relationships. If personal

information is publicly available, there is every possibility that it can be used to hurt or harm or threaten relationships. Finally, privacy is necessary for a person's personal identity. If personal information is publicly available without due and just restrictions, it can be used to wrongfully impersonate an individual. Privacy and data protection is necessary to guard an individual from cybercrimes/ cyber frauds and impersonation of various forms and types. It has been seen that personal information of various types and forms are available in the dark web which are then used to harm an individual through threat, inducement, blackmailing, etc. All these reasons make privacy and data protection necessary.

2. **Challenges to privacy and data protection in today's world:** The digital era has brought with it many new challenges related to the right to privacy and data protection. One such challenge is the increasing use of technology by criminals and terrorists to track and spy on individuals. At the other spectrum, it is also argued that the State is increasingly intruding into personal freedom through the use of technology in various forms. Coupled with the rapid advancement of technology is the increasing deployment and usage of artificial intelligence (AI), machine learning (ML) and other forms of automation to potentially and adversely impact the privacy of individuals.

3. **Need to have mechanisms for personal data and privacy for court officials**: Apart from the need to put in place physical security and security of court premises which has been adequately dealt by the Hon'ble Supreme Court in its discussions and subsequently in its order dated 11th August, 2023 in the Writ Petition (Criminal) No.99/2015 titled **"Pradyuman Bisht Vs. Union of India & ors.**', it has also put the onus on the High Courts to frame guidelines on data protection and its privacy. As a follow up, the present Committee was constituted for drafting the guidelines for the High Court and the District Courts in the State. The Committee discussed various aspects of data protection and its privacy features in its meetings held on 28.08.2023, 20.09.2023 and 22.09.2023 and further attempted to put in place a draft guidelines.

4. For the purpose of the present guidelines, it was decided to first of all define "personal data" in the following manner which will constitute:

(i) any information and facts to include personal data like bio-data, bank details, information as available in the service book, remuneration, etc of the judges and judicial officers which are available in digital form or in non-digital form maintained by the Registry and District Courts;

(ii) case related data and information which are of sensitive nature which is under consideration by the judges and judicial officers;

(iii) any data and information conveyed by the judges and judicial officers to constitute personal data which are sensitive in nature.

5. Based on the above limited definition of personal data, it was also contemplated that only the personal data of judges and judicial officers in the State would be covered under these Guidelines. Thereafter, the following guidelines were drafted by the Committee for consideration and approval:

a) **Sharing of personal data:** Any data as defined under these Guidelines shall be accessed and shared only if consent in writing is conveyed for the same by the official concerned. However, in cases where legal proceedings and investigations or where the life and liberty of the concerned person is involved, certain personal data as necessary shall be processed and / or shared without consent. Notwithstanding this, due care shall be carried out at every stage to ensure that such personal information and data are maintained in such a manner to ensure adequate privacy and avoid undue public exposure which may threaten the privacy, life and liberty of the person concerned. The purpose and means of processing and sharing of personal data of the concerned persons should be duly recorded to ensure transparency, clarity and sufficiency.

b) **Key principles that apply to the processing of personal data:** Personal data shall be processed lawfully, fairly and in a transparent

manner in relation to the data subject. The key principles that apply to the processing of personal data shall include lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality (security), and accountability.

c) **Implementation of a proper security system (data encryption) to prevent misuse of personal data and information and maintain privacy:** Whenever the implementation of security software is put in place, the maintenance of personal data should be in such manner which would include user activity monitoring, automated access management, notifications on security events, audit measures and such other mechanisms to ensure adequate, sufficient and optimum level of data protection and privacy.

d) **Maintenance of records of personal data and information:** The Registry / District Court shall appoint an official to be designated as "Data Protection Officer" (DPO) of adequate level and such staff (if required) to determine the purpose and means of processing of personal data. Such a DPO and staff should be an official from the existing pool of permanent officials and staff. The DPO will be responsible for all such matters, inter alia, which would include (i) maintaining and recording all such personal data of the judges and judicial officers, (ii) carrying out periodic review of the mechanisms to ensure adequate data protection and privacy, (iii) reporting any lapses or shortcomings in the mechanism and system, (iv) recommending/ suggesting steps to improve the mechanism and system to ensure data protection and privacy. He would also be responsible to ensure that any data collection and processing activities are carried out in a transparent and fair manner. Further, he should be able to explain to the Judges and Judicial Officers why their data is being collected and how it will be used and the purpose of such usage. As and when called for, the Data Protection Officer will present the status of the kinds and types of personal data that is being maintained.

e) **Data protection impact assessment:** In order to ensure that proper mechanism is available in place with regard to storing, compiling, processing and sharing of personal data of the concerned persons and maintaining privacy of such information and data, it is mandatory that there should be a six-monthly assessment or review. At the High Court level, such review will be done by the Registry and at the District level, it will be done at the level of the District & Sessions Judge. Review will invariably include listing of the kinds and types of personal data being collected and stored, processing activities of such data along with the nature and purpose, steps taken to ensure personal data protection and privacy. A summary report will be prepared individually and shared with the concerned official,s the list of personal data being stored and how it was shared during the period of review. If during such reviews and assessment, the Registry/District Courts comes across any shortcomings in the processes and manner how such data was used and shared, it shall make recommendations for implementation. It will also look into any lapses that may have occurred during the stages of implementation. It will be the duty of the DPO to prepare and present a detail report of the working of data protection during such reviews.

f) **Setting up of grievance redressal mechanisms to address complaints:** Whenever an information in writing is received from the concerned judges and/ or judicial officers regarding the misuse of personal data and information or any such related complaints, it should be duly acknowledged and immediate steps be taken to resolve it and convey the steps that have been taken. It shall be the duty of the DPO to attend and resolve such grievances. If there is any lapses in the maintenance of such personal data and information, inquiry should be made into it and responsibilities will be fixed.

g) **Assessment and review**: As part of the implementation process of these Guidelines, the Registry / District Court will undertake a thorough assessment of the level, types and kinds of personal data being presently available and maintained. At the District level, the District & Sessions Judge will make such an assessment to have a full understanding of the

level, types and kinds of personal data being available and maintained. This assessment should be carried out as the first step in the implementation of these Guidelines. As part of the assessment process, the availability of personal data will be studied and categorised as "not sensitive", "sensitive" and "highly sensitive" personal data. This lists of personal data made under such a categorisation or the prospective list of such data will then be communicated to the respective judges and judicial officers. The Data Protection Officer will then ensure that he puts in place a mechanism and system to fully protect such personal data and information.

***