Obligation to comply with data protection requirements under the General Data Protection Regulation (GDPR) and local privacy laws

1. The Employee shall process personal data,that was accessed withinthe term of his or her employment with Luxoft India LLP (the “Company”), in accordance with the following principles:
   1. The Employee shall in particular not collect personal data,or any special categories of such data, without approval of the Data Protection Officer at[DPO@luxoft.com](mailto:DPO@luxoft.com) (hereinafter – DPO). The Employee shall contact the DPO prior to collection when in doubt of the legal groundsapplicable thereto.
   2. The Employee shall strictly follow all corporate global and local privacy policies and procedures, established for the data processing activity, in which Employee participates, for example to collect the data subject’s consent in accordance with the corporate recruitment procedure(via E-consent portal, website forms, recorded calls, etc.).
   3. The Employee shall ensure to only process personal data for the specified, explicit and legitimate purposes for which the personal data has initially been collected by the Company and its affiliates. The Employee is not allowed to further process personal data in a manner that is incompatible with or beyond those purposes or after leaving the Company. The Employee shall contact the DPOprior to processing when in doubt of the processing purposes.
   4. The Employee shall only process personal data which is necessary and relevant in relation to the processing purposes.
   5. The Employee shall ensure that the processed personal data is accurate and, where necessary, kept up to date. The Employee shall contact the data subject when in doubt of the accuracy of the personal dataprior to processing thereby.
   6. The Employee shall comply with the [Luxoft Group Data Protection Policy](https://luxproject.luxoft.com/confluence/pages/releaseview.action?pageId=59803250)at all times when processing personal data.
   7. The Employee shall review his/hercorrespondences, files and documents on a regular basis to assess whether the personal data accessible therein is no longer necessary for the purpose it was collected and should therefore be considered for deletion. Prior to deletion, the Employee shall check and adhere corporate [Document Retention Policy](https://luxproject.luxoft.com/confluence/pages/viewpage.action?pageId=116589078).
   8. The Employee shall keep personal data confidential and prevent unauthorized or unlawful access and accidental loss, destruction or damage, by using appropriate technical or organizational measures, e.g. using of corporate e-mail address, follow “clean desk” rule, taking away from printing devices,storage only on servers/clouds/devices belonging to the Company in accordance with the [Rules on Company information treatment by employees](https://luxproject.luxoft.com/confluence/pages/releaseview.action?pageId=59803827), guidance from DPOs .
   9. The Employee shall only give access to personal data to other employees or third parties on a “need to know” basis, i.e. to persons which need to process such personal data, e.g. based on their job description. In particular with regard to external third parties (i.e. not [Luxoft Group entities](https://www.luxoft.com/about-us/)), the Employee shall obtain approval of the DPO before transferring personal data to such external third party. The Employee shall follow the Company’s [Security Incidents Management policy](https://luxproject.luxoft.com/confluence/pages/releaseview.action?pageId=61820213#InformationSecurityOfficer) and advise from DPOs.
   10. The Employee shall immediately report any actual orsuspected personal data breach or any other event related to security of personal data, in accordance with the [Personal Data Breach Policy in Security Incidents Management](https://luxproject.luxoft.com/confluence/pages/releaseview.action?pageId=61820213#InformationSecurityOfficer).
   11. The Employee shall immediately notify DPO about upcoming:
   * projects involving personal data;
   * processing of personal data under client’s, supplier’s or other third party instructions;
   * transfers of personal data outside EU or outside its place of origin;
   * delegations of data processing to a third party;
   * transfer of employee’s/candidate’s personal data to clients, suppliers or other third party (except – business contacts and CVs of project team).
2. Breach of this obligation can be sanctioned with fines and/or imprisonment in accordance with applicable law. At the same time, a breach may constitute a breach of the employment contract obligations or special confidentiality obligations, which may entail disciplinary action or dismissal. Civil claims for damages can also arise from culpable breaches of this undertaking. The Employee’s confidentiality obligation resulting from the employment or service contract or separate agreements is not affected by this undertaking, which shall be read, deemed or construed as an essential obligation or term of such employment or service.
3. This obligation shall be a continuing obligation applicable for the protection of personal data accessed within the term of employment, after the termination of employment . For the avoidance of doubt, this is a perpetual obligation.
4. **Definitions*:***

**Personal data** means(i) any information that can be used to distinguish or trace an individual‘s identity, such as person’s name, date and place of birth, biometric records, mother’s maiden name, address, email address, telephone number, social security number, state identification or driver’s license numbers, account information, PIN numbers, access and security codes, login information; and (ii) any other information that is linked or linkable to an individual, such as information about a person’s sex, age, income, health or medical information, educational, financial and employment information.

**Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

|  |
| --- |
| Hyderabad, 22-05-2022  Place, Date |
| Chinnikrishna Darapureddy  Name of Employee |
| Chinnikrishna_Signature.png  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature of Employee |