NOTICE FOR INVITING APPLICATIONS FOR RECRUITMENT OF DATA PROTECTION OFFICER

Position	One (1) Data Protection Officer (DPO)
Number of posts	One (1) – UR
Type of Post	Contractual
Place of Posting	Mumbai
Period of Contract	The term of contract would initially be for a period of 3 (Three) years, further extendable by 2 (Two) years as per the Bank's discretion.
Essential Qualification	• Graduate in any discipline from a University / Institution recognised by the Government of India or approved by a Government regulatory body. Minimum 60% aggregate marks / equivalent Cumulative Grade Points Average (CGPA), in Graduation. The graduation course should be of a minimum 3-year full-time duration. • **Mandatory certification –** at least one of the following, valid as on the cut-off date: Certified Information Privacy Professional/Europe (CIPP/E), Certified Information Privacy Professional/Asia (CIPP/A), Certified Information Privacy Manager (CIPM) or Fellow of Information Privacy (FIP), awarded by the International Association of Privacy Professionals (IAPP); Certified Data Privacy Solutions Engineer (CDPSE), awarded by ISACA; DSCI Certified Privacy Professional (DCPP), DSCI Certified Privacy Lead Assessor (DCPLA) or DSCI Certified Data Protection Officer (DCDPO), awarded by the Data Security Council of India (DSCI); Certified Data Protection Officer (CDPO), awarded by PECB – the Provisional grade of this credential shall not be reckoned; • **Preferred (not mandatory)**: a post-graduate degree / diploma, or a degree in Law, Engineering, Computer Science / Information Technology, or a professional qualification such as CA / CS / MBA. • **Preferred additional certification (not mandatory):** CISA, CISM, CISSP, ISO/IEC 27701 Lead Implementer or Lead Auditor, ISO/IEC 27001 Lead Auditor.
Experience	• Minimum 15 years' post-qualification experience in an executive / managerial capacity in the corporate sector, preferably in the Banking, Financial Services and Insurance (BFSI) sector. • Of the above, a minimum of 5 years in a senior managerial or leadership role; and a minimum of 5 years in data privacy / data protection or closely allied disciplines – namely data governance and data management, information security with a data protection focus, legal or compliance work relating to data protection and outsourcing, operational or third-party risk management covering personal data, or governance, risk and compliance consulting on privacy engagements including experience in dedicated data

	privacy / data protection work, including programmes under the Digital Personal Data Protection Act, 2023, the GDPR, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, or an equivalent regime. • Demonstrated hands-on experience in the following: privacy policy and framework development; record of processing activities and data flow mapping; notice and consent design, including withdrawal and consent logging; data protection impact assessment; data principal / data subject rights fulfilment; personal data breach management and regulatory notification; third-party and vendor privacy risk assessment; cross-border data transfer assessment; privacy audits. • Experience of engaging with regulators and supervisory authorities, statutory and internal auditors, and of presenting to Board-level committees.
Age Limit	Should not be more than 50 years of age as on November 01, 2026.
Scope of Work	• To function as the Data Protection Officer of the Bank for the purposes of the Digital Personal Data Protection Act, 2023 and the Rules framed thereunder, and to be the person whose contact particulars are published by the Bank under Section 8(9) of the Act. In the event the Bank is notified as a Significant Data Fiduciary, to discharge the duties of the Data Protection Officer under Section 10(2)(a) of the Act. • To own the Bank's data privacy framework end to end – policy, processes, controls, assurance and reporting – and to lead the DPDP implementation programme to the statutory timeline, and thereafter to run it on a business-as-usual basis. • Coverage extends to all Groups at Head Office, domestic Regional / Representative Offices, overseas offices and subsidiaries of the Bank as applicable, and to personal data processed by third parties on behalf of the Bank. • To act as the single point of contact for Data Principals, for the Data Protection Board of India and for other regulators on data protection matters.
Key Skills Required	• Expert knowledge of Indian data protection law and practice, and working familiarity with global privacy regimes. • Ability to translate statutory obligations into implementable policies, standard operating procedures and system requirements. • Information lifecycle management – data discovery and classification, retention, archival and erasure.

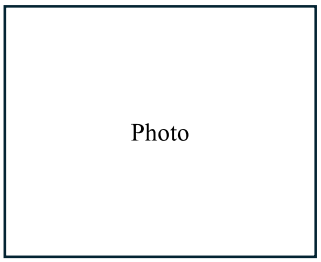
	• Privacy risk assessment – data protection impact assessment, third-party risk and cross-border transfer assessment. • Incident and personal data breach management, including notification to the regulator and to affected individuals within prescribed timelines. • Drafting skills – policies, privacy notices, consent artefacts and contractual data protection clauses. • Stakeholder management and the ability to influence across Business, Legal, Compliance, Information Technology, Human Resources, Risk Management and Internal Audit. • Board-level communication and report writing. • Training, awareness and change management. • Independence, integrity and the ability to hold a considered position on compliance matters.
Job Profile	• Report on data protection matters to the Board of Directors or a Committee of the Board, with direct and unrestricted access, while maintaining functional independence from the Information Technology and Information Security functions. • Formulate, obtain approval for and maintain the Bank's Data Privacy Policy together with supporting standards, procedures and guidelines, and keep them aligned to changes in law and regulation. • Establish and maintain the Bank's personal data inventory, Record of Processing Activities and data flow maps, and document the lawful basis for each processing activity. • Design and oversee the notice and consent architecture, including consent withdrawal, maintenance of consent and withdrawal logs. • Establish and operate the Data Principal rights process – access, correction and erasure, nomination and grievance redressal – within the timelines prescribed under the Act and the Rules. • Conduct and oversee data protection impact assessments; where the Bank is notified as a Significant Data Fiduciary, cause the annual data protection impact assessment and independent data audit to be carried out and the significant observations to be reported to the Data Protection Board of India. • Jointly with the Chief Information Security Officer, ensure that reasonable security safeguards are implemented and maintained to prevent personal data breaches, and lead the breach response process – including intimation to affected Data Principals without delay and submission of the detailed report to the Data Protection Board within the prescribed period.

	• Embed data protection requirements into the Bank's third-party risk management framework and into vendor and outsourcing contracts. • Assess, document and control cross-border transfers of personal data, including data processed at or accessed from the Bank's overseas offices. • Institutionalise privacy by design in new products, systems, processes and change initiatives, and clear them from a data protection standpoint. • Design and deliver data privacy training and awareness for employees, contractual staff and vendors. • Maintain the privacy risk register and report management information, key risk indicators and programme status to the management committees and to the Board or its Committee on a periodic basis. • Supervise the Deputy Data Protection Officer and the privacy team and coordinate the network of privacy champions across Groups. • Track legal, regulatory and supervisory developments in data protection; liaise with regulators and coordinate inspections, audits and regulatory submissions relating to personal data. • Any other duties assigned by the Bank from time to time in connection with data protection and privacy.
Compensation	• Rs. 26.71 lakh per annum with annual increments. The compensation has fixed and variable components in the ratio of 80:20. The compensation may increase as per the Bank's pay matrix for candidates having more work experience.
Last Date to Apply	• November 30, 2026
How to apply	• Eligible candidates may send their resume as per the attached format to hrm@eximbankindia.in with the subject line: **DPO Application: Mr./ Ms. (Full Name)**

The Bank will shortlist eligible candidates for personal interview at its office in Mumbai. Only shortlisted candidates will be informed regarding the interview. Candidates are requested to check their eligibility before sending their resumes as no correspondence will be made with ineligible candidates and candidates who are not shortlisted for the interview process.

Candidates will be shortlisted for interviews in the ratio of 1:10. A list will be drawn from among the candidates who meet all the prescribed eligibility criteria. In the event more than 10 candidates are found eligible, a shortlist will be drawn based on the percentage score at post-graduation examination. The Bank may, at its discretion, relax the eligibility criteria relating to experience, age, essential qualifications, and ratio for shortlisting candidates in the event of a limited response to the advertisement or an insufficient number of candidates being found eligible.

APPLICATION FORMAT FOR OFFICER – DATA PROTECTION OFFICER



PERSONAL DETAILS		
1.	Name	
2.	Date of Birth(dd/mm/yyyy)	
3.	Age as on November 01, 2026	
4.	Nationality	
5.	Category	
6.	Email Id	
7.	Mobile Number	
8.	Correspondence Address	
EDUCATION AND PROFESSIONAL QUALIFICATION		
1.	GRADUATION: Name of the college / University	
	Mode: Full Time/ Part Time	
	Year of Passing	
	Percentage of Marks	
2.	POST GRADUATION: Name of the college / University	
	Mode: Full Time/ Part Time	
	Year of Passing	
	Percentage of Marks	
3.	Mandatory Certification Name of the certification as per the advertisement	

	Year of Passing	
	Percentage of Marks/ Grade	
4.	ANY OTHER QUALIFICATION: Name of the college / University	
	Year of Passing	
	Percentage of Marks	
CAREER SUMMARY (Start with the latest / present)		
1.	Name of the Company	
	Position / Designation	
	Tenure (From / To)	
	Location	
	Key Responsibilities	
2.	Name of the Company	
	Position / Designation	
	Tenure (From / To)	
	Location	

	Key Responsibilities	
3.	Name of the Company	
	Position / Designation	
	Tenure (From / To)	
	Location	
	Key Responsibilities	
4.	Total number of post-qualification work experience in years	
5.	Total number of post-qualification work experience in a senior managerial or leadership role	
6.	Do you have a minimum of 5 years in data privacy / data protection or closely allied disciplines as per the advertisement?	

ADDITIONAL INFORMATION

1.	Current CTC (Annual)	
2.	Expected CTC (Annual)	
3.	Notice Period	
4.	Have you ever been convicted by a court of law? (Yes/No)	
5.	Any ongoing criminal/disciplinary proceedings? (Yes/No)	
6.	Are you related to any employee of the Bank? (Yes/No)	

DECLARATION

I hereby declare that all information provided above is true and correct to the best of my knowledge. I understand that any false information may lead to disqualification from the recruitment process.

Date: _____

Signature: _____

NOTICE FOR INVITING APPLICATIONS FOR RECRUITMENT OF A DEPUTY DATA PROTECTION OFFICER

Position	One (1) Deputy Data Protection Officer (Deputy DPO)
Number of posts	One (1) – UR
Type of Post	Contractual
Place of Posting	Mumbai
Period of Contract	The term of contract would initially be for a period of 3 (Three) years, further extendable by 2 (Two) years as per the Bank's discretion.
Essential Qualification	• Graduate in any discipline from a University / Institution recognised by the Government of India or approved by a Government regulatory body. Minimum 60% aggregate marks / equivalent Cumulative Grade Points Average (CGPA), in Graduation. The graduation course should be of a minimum 3-year full-time duration. • **Mandatory certification –** at least one of the following, valid as on the cut-off date: Certified Information Privacy Professional/Europe (CIPP/E); Certified Information Privacy Professional/Asia (CIPP/A); Certified Information Privacy Manager (CIPM) **OR** Fellow of Information Privacy (FIP), awarded by the International Association of Privacy Professionals (IAPP); **OR** Certified Data Privacy Solutions Engineer (CDPSE), awarded by ISACA; DSCI Certified Privacy Professional (DCPP), DSCI Certified Privacy Lead Assessor (DCPLA) **OR** DSCI Certified Data Protection Officer (DCDPO), awarded by the Data Security Council of India (DSCI); Certified Data Protection Officer (CDPO), awarded by PECB – the Provisional grade of this credential shall not be reckoned; • **Preferred:** a post-graduate degree / diploma, or a degree in Law, Engineering, Computer Science / Information Technology, or a professional qualification such as CA / CS / MBA. • **Preferred additional certification:** CISA, CISM, CISSP, ISO/IEC 27701 Lead Implementer or Lead Auditor, ISO/IEC 27001 Lead Auditor.
Experience	• Minimum 5 years' post-qualification experience in an executive / managerial capacity in the corporate sector, preferably in the Banking, Financial Services and Insurance (BFSI) sector. • Of the above, a minimum of 2 years in data privacy / data protection or closely allied disciplines – namely data governance and data management, information security with a data protection focus, legal or compliance work relating to data protection and outsourcing, operational or third-party risk management covering personal data, or governance, risk and

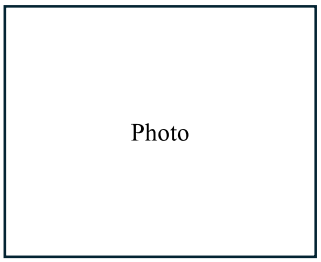
	compliance consulting on privacy engagements including experience in dedicated data privacy / data protection work, including programmes under the Digital Personal Data Protection Act, 2023, the GDPR, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, or an equivalent regime. • Demonstrated hands-on experience in the following: record of processing activities and data flow mapping; notice and consent implementation; data protection impact assessment; data principal / data subject rights fulfilment; personal data breach handling; third-party and vendor privacy risk assessment; privacy training and awareness; privacy audit support. • Working knowledge of the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025; exposure to the GDPR or other global privacy regimes is desirable. • Experience of supporting internal, statutory or regulatory audits and of preparing management information and compliance reporting.
Age Limit	Should not be more than 40 years of age as on November 01, 2026.
Scope of Work	• To assist the Data Protection Officer in discharging the obligations of the Bank under the Digital Personal Data Protection Act, 2023 and the Rules framed thereunder, and to act for the Data Protection Officer during his or her absence. • To carry out the day-to-day operation of the Bank's data privacy framework – maintenance of records, processing of data principal requests, assessments, monitoring and reporting. • To serve as the working-level point of contact for Groups, Regional and Overseas Offices and vendors on data protection matters, and to coordinate the privacy champion network. • Coverage extends to all Groups at Head Office, domestic Regional / Representative Offices, overseas offices and subsidiaries of the Bank as applicable, and to personal data processed by third parties on behalf of the Bank.
Key Skills Required	• Sound working knowledge of the Digital Personal Data Protection Act, 2023 and the Rules, and the ability to apply them to day-to-day banking processes. • Documentation discipline – maintenance of inventories, registers, assessment records and audit evidence. • Data discovery, classification, retention and erasure practices. • Conduct of data protection impact assessments and vendor privacy assessments.

	• Handling of data principal requests and grievances with accuracy and within timelines. • Drafting of procedures, checklists, privacy notices and training content. • Coordination and follow-up skills across multiple Groups and Departments. • Preparation of management information, dashboards and compliance reports. • Discretion in handling confidential and personal information.
Job Profile	• Report to the Data Protection Officer and assist in the implementation and running of the Bank's data privacy programme. • Maintain the personal data inventory, the Record of Processing Activities and the data flow maps and keep them current through periodic review with Groups. • Operate the Data Principal rights process on a day-to-day basis – receipt, identity validation, coordination with the concerned Group, response and closure within prescribed timelines – and maintain the rights and grievance registers. • Maintain the consent and consent-withdrawal logs and monitor that notice and consent requirements are being met across the Bank's channels. • Carry out data protection impact assessments and privacy reviews of new and existing products, systems, processes and change initiatives, and track remediation of findings to closure. • Conduct privacy risk assessments of vendors and service providers, and verify that the prescribed data protection clauses are incorporated in contracts. • Support the personal data breach process – initial assessment, evidence collation, preparation of the intimation to affected Data Principals and of the report to the Data Protection Board of India – in coordination with the Information Security and Information Technology functions. • Monitor compliance with the data retention and erasure schedule, and follow up on overdue deletion and archival actions. • Assist in the annual data protection impact assessment and independent data audit, and in internal, statutory and regulatory audits and inspections, including preparation of responses and compliance of observations. • Deliver data privacy training and awareness sessions for employees, contractual staff and vendors, and maintain training records.

	• Prepare periodic management information, key risk indicators and programme status reports for the Data Protection Officer, management committees and the Board or its Committee. • Maintain the data privacy document set – policy, standards, procedures, templates and registers – under version control. • Any other duties assigned by the Bank or by the Data Protection Officer from time to time in connection with data protection and privacy.
Compensation	• Rs. 18.38 lakh per annum with annual increments. The compensation has fixed and variable components in the ratio of 80:20. The compensation may increase as per the Bank's pay matrix for candidates having more work experience.
Last Date to Apply	• November 30, 2026
How to apply	• Eligible candidates may send their resume as per the attached format to hrm@eximbankindia.in with the subject line: Deputy **DPO Application: Mr./ Ms. (Full Name)**

The Bank will shortlist eligible candidates for personal interview at its office in Mumbai. Only shortlisted candidates will be informed regarding the interview. Candidates are requested to check their eligibility before sending their resumes as no correspondence will be made with ineligible candidates and candidates who are not shortlisted for the interview process.
Candidates will be shortlisted for interviews in the ratio of 1:10. A list will be drawn from among the candidates who meet all the prescribed eligibility criteria. In the event more than 10 candidates are found eligible, a shortlist will be drawn based on the percentage score at post-graduation examination. The Bank may, at its discretion, relax the eligibility criteria relating to experience, age, essential qualifications, and ratio for shortlisting candidates in the event of a limited response to the advertisement or an insufficient number of candidates being found eligible.

APPLICATION FORMAT FOR OFFICER – DEPUTY DATA PROTECTION OFFICER



PERSONAL DETAILS		
1.	Name	
2.	Date of Birth(dd/mm/yyyy)	
3.	Age as on November 01, 2026	
4.	Nationality	
5.	Category	
6.	Email Id	
7.	Mobile Number	
8.	Correspondence Address	
EDUCATION AND PROFESSIONAL QUALIFICATION		
1.	GRADUATION: Name of the college / University	
	Mode: Full Time/ Part Time	
	Year of Passing	
	Percentage of Marks	
2.	POST GRADUATION: Name of the college / University	
	Mode: Full Time/ Part Time	
	Year of Passing	
	Percentage of Marks	
3.	Mandatory Certification Name of the certification as per the advertisement	

	Year of Passing	
	Percentage of Marks/ Grade	
4.	ANY OTHER QUALIFICATION: Name of the college / University	
	Year of Passing	
	Percentage of Marks	
CAREER SUMMARY (Start with the latest / present)		
1.	Name of the Company	
	Position / Designation	
	Tenure (From / To)	
	Location	
	Key Responsibilities	
2.	Name of the Company	
	Position / Designation	
	Tenure (From / To)	
	Location	

	Key Responsibilities	
3.	Name of the Company	
	Position / Designation	
	Tenure (From / To)	
	Location	
	Key Responsibilities	
4.	Total number of post-qualification work experience in years	
5.	Of the above, do you have a minimum of 2 years of experience in data privacy / data protection or closely allied disciplines as per the advertisement?	

ADDITIONAL INFORMATION

1.	Current CTC (Annual)	
2.	Expected CTC (Annual)	
3.	Notice Period	
4.	Have you ever been convicted by a court of law? (Yes/No)	
5.	Any ongoing criminal/disciplinary proceedings? (Yes/No)	
6.	Are you related to any employee of the Bank? (Yes/No)	

DECLARATION

I hereby declare that all information provided above is true and correct to the best of my knowledge. I understand that any false information may lead to disqualification from the recruitment process.

Date: _____

Signature: _____