Eskom Pension and Provident Fund ("EPPF")

Operator Privacy Due Diligence Form

The completion of this form is guided by the EPPF Operator Privacy Due Diligence Procedure.

Operators to complete the Due Diligence Results column and then submit the completed form together with supporting documentation to the Administrator, Legal and the Deputy information Officer for evaluation and approval, prior to finalising the contract with the Operator. In instances where a contract already exists, Operators need to evaluate the existing contract against the set criteria.

Operator Privacy Due Diligence Criteria

The following minimum criteria that should be taken into account when conducting the Privacy Due Diligence and formulating the contract with the Operator. Additional criteria may be added, if required.

Subject	Criteria	Due Diligence Results' (To be completed by the Operator)	Evaluation - Items Requiring Action
Contract			
Security Safeguards	1. Clause requiring that reasonable (in terms of prevailing good practice) security safeguards are in place for EPPF personal Information processed, whether electronic or paper-based.	What security safeguards does your organisation have in place to protect PI? Provide evidence.	
	2. Clause requiring that the Operator implement any additional security measures required in terms of agreement with EPPF from time to time.	Related to the above, do you foresee or plan that additional measured may be required?	
Confidentiality	3. Clause requiring the confidentiality of all EPPF Personal Information processed by the Operator.	Provide a statement that PI will be kept confidential.	
	4. Clause requiring that no EPPF Personal Information may be disclosed to any 3rd Party without the prior written permission of EPPF.	Provide a statement that PI will not be disclosed to 3rd parties.	
Access Control	5. Clause requiring EPPF approval of all access requests for Employee or third-party access to Operator applications and data involving EPPF data or Personal Information.	What access control measures to PI does your organisation have in place? Provide evidence.	

Subject	Criteria	Due Diligence Results' (To be completed by the Operator)	Evaluation - Items Requiring Action
Privacy compliance	6. Clause requiring that the Operator complies with POPIA (including the POPIA Regulations and any future amendments to POPIA) when processing Personal Information, Special Personal Information and Children's Personal Information.	What POPIA compliance documents, standards and measures does your company have in place?	
Processing	7. Clause requiring written authorisation by EPPF before Operator may process any EPPF Personal Information.	Statement that you will not process PI without authorisation.	
	8. Is a documented service level agreement in place with the Operator?	Provide evidence of SLA.	
	9. Is the standard EPPF Data Processing Agreement in place with the Operator?	Provide evidence of Agreement if relevant	
Jurisdiction	10. Determine all jurisdictions in which the Operator will process EPPF Personal Information, including the use of Cloud services and/or storage in international jurisdictions.	State all jurisdictions where you will process EPPF PI.	
	11. Clause requiring that EPPF is notified in writing as to the EPPF Personal Information (broken down into Personal Information, Special Personal Information and Children's Personal Information) that is to be processed by the Operator, and in which jurisdictions.	State which EPPF PI will be processes as part of the agreement.	
	12. Evaluate the compatibility of each jurisdiction in terms of adequacy of data protection law (as compared to the POPIA Act).	What data protection measures you're your organisation have in place? Provide evidence.	
	13. Clauses requiring immediate reporting of any change in jurisdiction by the Operator or any other sub-Operators processing EPPF Personal Information on the Operator's behalf.	Statement that any change in jurisdiction will be reported.	

Subject	Criteria	Due Diligence Results' (To be completed by the Operator)	Evaluation - Items Requiring Action
Cross-border transfers	14. Clause governing cross-border transfers of EPPF Personal Information processed by the Operator. All cross-border transfers of Personal Information, Special Personal Information and children's Personal Information must be in compliance with the POPIA Act, and data subject written consent must be obtained as and when required by POPIA. Particular care must be taken when transferring Personal Information to jurisdictions that do not have data protection law equivalent to POPIA, and when transferring Special Personal Information or children's Personal Information.	How would you handle cross-border transfer of EPPF PI – if relevant?	
Breach of Personal Information (including special Personal Information and Children's Personal Information)	15. Clause requiring telephonic reporting of Personal Information breach or suspected breach to EPPF immediately (within 1 hour) upon identification thereof. Telephonic report must be promptly followed up by comprehensive written report detailing the breach.	Statement that any breach will be reported immediately.	
	16. Clause addressing penalty payment of **1 Million Rand** in the event of a failure to reporting a breach or suspected breach by telephone within 1 hour of detection.	Statement that you are aware of the penalty payment.	
	17. Does the breach clause specify full disclosure of the nature and scope of the breach; all EPPF Personal Information and Special Personal Information affected or potentially affected, including names of affected Data Subjects; measures taken to contain the breach and measures taken to prevent future breaches.	What measures does your organisation have in place to contain any PI breach?	
	18. Clause stipulating that the Operator may not contact EPPF Data Subjects directly in the event of a breach. EPPF will perform this action and will inform the Information Regulator.	Statement that you will not contact data subjects in the event of any breach.	
	19. Clause agreeing that EPPF will be allowed to participate fully in the forensic investigation of any breach involving EPPF Personal Information.	Statement that EPPF will be allowed to participate in investigating of any breach that may occur.	

Subject	Criteria	Due Diligence Results' (To be completed by the Operator)	Evaluation - Items Requiring Action
Secondary Operators processing EPPF Personal Information	20. Clause requiring that the Operator obtains written approval from EPPF prior to engaging the services of any third-party or sub-contractor to assist in providing the contracted services to EPPF. This will include the identity and location of the subcontractor or Third Party and detail of all the jurisdictions that they may process EPPF Personal Information in.	Will third party services be required? Provide details.	
	21. Clause requiring that a sub-Operator may not, in turn, use a third party to process EPPF Personal Information. If this occurs, it will be considered to be a breach of EPPF Personal Information.	Statement that your organisation will take responsibility for the processing of PI by yourself and/or any third party.	
	22. Clause requiring that adequate back-to-back contracts and/or agreements be in place between EPPF, the Operator, and any Operator sub-contractors or third parties. These must mirror the contract between the Operator and EPPF, thus adequately addressing POPIA compliance.	Statement that contracts are in place with third parties. Provide copies.	
	23. Clause requiring disclosure to the Operator and EPPF of every jurisdiction in which each sub-Operator will process EPPF Personal Information, including prior written notification when jurisdictions change.	Statement that jurisdiction changes will be disclosed.	
	24. Clause requiring that back-to-back agreements require immediate (within one hour of detection) disclosure of breaches or suspected breaches of Personal Information? The Operator will be subject to penalties for any failure of their sub-Operators to report.	Statement that any breach in back-to-back agreements will be reported immediately. Acknowledgement of penalties in place.	
	25. Clause requiring that EPPF is notified in writing as to the EPPF Personal Information (broken down into Personal Information, Special Personal Information and Children's information) that is to be processed by each sub-Operator, and in which jurisdictions.	Statement on PI that will be processed by every sub-operator.	
Retention and destruction of records	26. Clauses addressing Personal Information retention requirements for EPPF Personal Information processed by the Operator.	Statement that PI retention requirements will be adhered to.	

Subject	Criteria	Due Diligence Results' (To be completed by the Operator)	Evaluation - Items Requiring Action
	27. Clauses in place addressing the return and/or destruction of EPPF Personal Information in the event that the contract is terminated, taking into account the retention period that the Operator has to retain the information for legal purposes.	Statement that PI will be returned or destroyed when contract is terminated.	
	28. Clause in place that addresses the secure and permanent destruction of Personal Information once no longer required.	Statement that PI will be destroyed when no longer required.	
	29. Clause in place that addresses the return and/ or destruction of EPPF Personal Information held by a sub-Operator in the event that the contract is terminated between EPPF and the operator, and/or between the Operator and the sub-Operator.,	Statement that PI held by sub-contractors will be handled according to EPPF requirements.	
Termination of contract	30. Clause requiring that all EPPF Personal Information / records containing Personal Information, are promptly returned to EPPF on termination of contract, including all Personal Information in the possession of a third party or sub-contractor of the Operator. NB: This will exclude any records that the Operator is required to retain for a period specified by law.	Statement that any PI will be returned to EPPF on termination of the contract.	
	31. Clause requiring that EPPF be provided with destruction certificates of all Personal Information that was destroyed on termination of contract.	Statement that EPPF will be provided with destruction certificates within a specific time period.	
	32. Termination clauses must address the Operator as well as any sub-Operators.	So third parties should also return/destroy any PI they hold on termination of contract	
Collection of Personal Information	33. Clauses addressing collection of Personal Information on behalf of EPPF: The Operator will collect Personal Information directly from the data subject unless otherwise directed in writing by EPPF, or unless the Personal Information is provided by EPPF. The operator will ensure that consent is obtained from the data subject and that adequate notice is given to the data subject.	Statement that consent will be obtained from data subject for collection of PI.	

Subject	Criteria	Due Diligence Results' (To be completed by the Operator)	Evaluation - Items Requiring Action
Data Subject Participation	34. Clause specifying that if Data Subjects require access, correction or deletion, or object to the processing of their Personal Information by the Operator or a sub-Operator, this must be directed to EPPF to be handled in terms of the PAIA Manual on EPPF's website.	Statement that data subject requirements will be directed to EPPF.	
Monitoring and reporting	35. Clause requiring that the Operator complete and submit an annual Privacy Compliance Self-assessment to EPPF (on the form supplied by EPPF).	Completed Self-Assessment Form.	
	36. Clause detailing the regular reporting required from the Operator regarding the security safeguards in place to protect EPPF Personal Information.	Security safeguard report.	
	37. Clause detailing any other regular reporting requirements from the Operator regarding POPIA compliance.	Mention other reports that will be provided.	
	38. Clause detailing regular reporting requirements in terms of service level agreement/s.	SLA on reports.	
	39. Clause detailing regular reporting in terms of data Processing requirements.	SLA on reports.	
	40. Clause detailing regular reporting detailing EPPF Employees and Operator personnel that have access to EPPF applications and data processed by the Operator (or sub-Operator) on EPPF's behalf.	SLA on reports.	
	41. Clause detailing regular reporting on the outcome of attack and penetration testing and security vulnerability assessments of the operator or sub-Operators.	SLA on reports.	
	42. Cause detailing the regular submission of applicable independent third-party audit and/or certification of security safeguards and business and/or IT controls, such as ISAE 3402 / SSAE 18, ISO27001/2 certification.	SLA on reports.	

Subject	Criteria	Due Diligence Results' (To be completed by the Operator)	Evaluation - Items Requiring Action
Sub-Operator Privacy Due Diligence	43. Clause requiring that the Operator conduct a Privacy Due Diligence of every sub-Operator that will process EPPF Personal Information, and that the Due Diligence findings be submitted to the EPPF. Thereafter, written approval must be obtained from the EPPF prior to transferring any EPPF Personal Information to the sub-Operator.	This form….	
Operator self-assessment	44. Clause requiring that the Operator and each sub-Operator complete and submit the "Operator and Annual Privacy Compliance Self-assessment".	Same as 35	
Auditing	45. Clause specifying EPPF's right to audit the records and controls governing processing of EPPF Personal Information by the Operator.	Statement that EPPF has the right to audit records and controls.	
Indemnity	46. Clause that indemnifies EPPF against any loss, damages, claims, penalties, fines and/or any other cost (including legal fees) that EPPF may suffer due to failure by Operator or a sub-Operator to comply with the POPIA Act and/or the contract, service level agreement or data processing agreement with the Operator.	Statement that indemnifies EPPF against loss or damage.	
Service Level Agreement			
Service Level Agreement	47. Does the Service Level Agreement (SLA) specify performance metrics, reporting requirements and the reporting schedule?	Yes/No/Not applicable	
	48. Does the SLA include POPIA / Privacy metrics and reporting requirements and reporting schedule?	Yes/No/Not applicable	