RFP 03/2021: PROVISION OF PROFESSIONAL SERVICES RELATING TO THE PROTECTION OF PERSONAL INFORMATION ACT NO. 4 OF 2013

QUESTIONS AND ANSWERS

#	QUESTION	SARS RESPONSE
1	Due to the pandemic and virtual working, please could we sign and complete the bid document electronic?	Kindly note that SARS does not decide for bidders on the method used to sign the necessary bid submission documents. However, with reference to acceptable method of submission of all bid proposals, kindly refer to paragraph 10.2 to 10.7 of the main RFP document.
2	We want to confirm whether you require of the service provider to perform data discovery and mapping or whether the service provider needs to review the existing data discovery or mapping that was performed.	(i) The service provider to engage various business units to ascertain what kind of personal information they process; (ii) Whether they are the primary custodian of such personal information; (iii) For what purpose do they process personal information; (iv) Who do the primary custodian share personal information with internally (i.e. secondary processer) and for what purpose do they share; (v) Who is the recipient of personal information externally and for what purposes is it shared with external stakeholders (vi) Where shared with external stakeholders, whether written contracts are in place or not.
3	Does SARS have any existing data discovery and data flow mapping tools (e.g. OneTrust, TrustArc or BigID) that the service provider can use or do you require the service provider to provide for such tools and should the related costs for the tools (licence fees, etc.) be included in the costing.	SARS does not have the tools, especially those mentioned. The Process will be manual in relation to this phase and there cannot be an expectation that this is already automated. The service providers could make recommendations as part of the gap analysis and recommendations report.
4	Does SARS have a data classification policy and standards?	Yes

#	QUESTION	SARS RESPONSE
5	Has the the classification policy been applied to all sensitive data and/or PII.	Yes
6	Is the scope for both structured and unstructured discovery of PII.	The scope is for detailed Personal Information Impact Assessment as per RFP, yes this would include both structured and unstructured data. Engagement during workshops should help shed more light on the status quo.
7	Is it expected that the successful bidder will be providing privacy services for the full duration of 12 months or is this the maximum appointment period?	The Contract duration is 12 months maximum, kindly refer to the technical evaluation criteria template for further detail on this. The Scope is as per RFP.
8	Is the nature of the audit to test the adequacy of design of SARS's privacy controls; to test the effectiveness of implementation of the privacy controls or a combination of both design and effectiveness testing?	• The requirement is to assess the controls not to test. • The service provider to engage various business units to ascertain what kind of personal information they process; • Whether they are the primary custodian of such personal information; • For what purpose do they process personal information; • Who do the primary custodian share personal information with internally (i.e. secondary processer) and for what purpose do they share; • Who is the recipient of personal information externally and for what purposes is it shared with external stakeholders • Where shared with external stakeholders, whether written contracts are in place or not.
9	Has SARS conducted recent cyber and information security assessments where reliance can be placed?	Yes
10	Is there an expectation that a privacy information asset register is developed across all SARS business areas?	No, please refer to the Scope of the RFP. For now the gap analysis will suffice. This can be part of the recommendations that the SP can recommend to SARS.
11	Are IT and information security managed under centralised functions or is it more decentralised across business areas?	IT Security and Information Security are centralised and managed by 2 business functions

#	QUESTION	SARS RESPONSE
12	Please confirm whether there is an expectation to test implementation of controls at a branch level?	The requirements is to assess controls not to test controls.