External Third-party Control Obligations

Data Privacy

Version 7.3 Dated August 2024

Control Title	Control Description	Why this is important
1. Permitted Purpose	The third party must only process the personal information in line with the obligations of the order/agreement. Personal information is processed by the third party were permitted by law and for a specified, explicit and lawful purpose and not processed in a way incompatible with that purpose. This must follow Absa's requirements and local legislation.	Third parties must follow Absa's instructions so that personal information is only processed for the purpose specified by Absa, failure to do so will result in a violation of the law and could result in penalties and reputational damage.
2. Transparency and Openness	Where the third party is acting as a data controller/responsible party the third party must warrant that it has an effective data privacy governance process in place and has a lawful ground for processing. The third party must also have appropriate governance process in place such as a data privacy policy framework including but not limited to, a privacy notice to notify the data subject of the way their personal information is processed. The Third party must have an information officer/ data privacy officer registered with the applicable authority (if applicable in the country of their jurisdiction)	Absa and the third party must act responsibly and in line with applicable data privacy legislation to ensure that data subjects are informed of processing of their personal information.
3. Appropriate Security	The third party must implement and execute appropriate and sufficient technical and procedural security and organizational controls to prevent personal information from being accidentally or deliberately compromised, damaged or lost.	Third parties must appropriately protect personal information against accidental or deliberate unauthorized disclosure, misuse or loss to prevent damage to Absa's clients, customers, directors, third parties and employees, and so that Absa will not violate laws in most countries where it operates.
4. Information Retention	Personal information where the third party is an operator/processor of Absa must only be retained for as long as it is used to provide the service to Absa, and in line with Absa's Data Retention and Destruction policy.	Third parties must adhere to the clauses in the agreement's exit provisions on the return of Absa personal information. In the absence of any specific provision, the information must be deleted on termination of the contract, unless there is an applicable local law preventing this.
5. Effective Reporting	Effective mechanisms must be put in place to detect, report and remediate the unauthorized disclosure, misuse or loss of personal information or similar breach. The Third party must inform Absa of a breach immediately (within 24 hours, or as agreed in the Order or Agreement) upon discovery of the breach and notify Absa of the root cause of the incident and the steps taken to prevent future reoccurrence of a similar nature. Any data breach notifications to appropriate regulators. customers will be communicated to and agreed with Absa prior to publication of the notifications.	The effective and efficient reporting of information breaches to Absa is essential to ensuring appropriate responses and to manage the possible escalation of events to respective regulators and mitigate consequences for customers.

6. Documented Standards	The third party must annually update data privacy policies and processes based on applicable laws, which demonstrate organizational compliance with privacy governance requirements; and are linked to proven contractual enforcement mechanisms; and are regularly communicated to all staff. The Third Party's policies, processes and procedures align with applicable privacy legislation in all respects with regards to the processing of personal information and should	Updated policies and procedures with detailed individual roles and responsibilities are necessary to determine if third party performance meets applicable legislative requirements, and Absa's standards and if third party uses them to regularly communicate with staff and enforce them against staff who have contractual confidentiality and privacy obligations to comply with them during and after their employment.

	applicable legislation changes significantly, they would bring it to Absa's attention as this may require an amendment to the Agreement. The Third party must ensure that staff who deal with personal information are sufficiently trained on data privacy. The Third party must follow due process in terms of aligning with applicable privacy legislation to notify relevant regulators of their processing activities, as well as obtaining prior authorization, where required.	
7. Privacy Awareness Training	Privacy training and awareness is rolled out to staff to make them aware of internal data privacy governance processes and policies.	Training and awareness are necessary to ensure third party personnel are aware of their roles and responsibilities pertaining to the handling of personal information.
8. Data Subject Requests and Complaints	If the third party receives data subject access requests and complaints from data subjects pertaining to personal information process in terms of the agreement, the third party must have processes in place, aligned with applicable legislation, to: – manage challenges raised on the accuracy of information subject personal information, – manage a data subject's objection to the processing of their personal information – manage complaints raised by the data subjects in the event of their privacy rights being breached The third party must warrant that where a data subject's rights have been exercised in relation to personal information processed by the third party on behalf of Absa, we are notified of the matter and will respond in accordance with applicable privacy legislation. The third party must notify Absa as soon as reasonably possible if a complaint is raised against Absa so that we are able to respond accordingly. Where legislation requires, the third party should have a Promotion of Access to Information Manual, or Freedom of Information process in place.	Replying to or forwarding data subject requests in respect of their personal information and for any other requests or complaints relating to Absa's use of their personal information is necessary to comply with Absa's legal requirements in terms of applicable legislation and to ensure Absa responds to customer complaints timeously.
9. Processing Changes/ Sub Processing and Onward Transfers	Personal information processing changes should be agreed upon by the parties before change is implemented. Any further processing of personal information is forbidden unless explicit consent is obtained from Absa to do so. Where personal information is transferred onward to a sub-processor, Absa must be made aware of this transfer, agree to it in writing and the agreement with the sub-processor must be aligned to Absa's requirements and the requirements of this agreement. When the onwards transfer of information results in the cross-border transfer of information, binding corporate rules or a data transfer agreement must be in place between the Third party and any other entities within their organization. Absa must be notified of jurisdictional transfers of information to jurisdictions who do not have adequate data privacy protection in place.	It is essential that Absa is notified of any changes to sub processors and onward transfers, whether cross-border or within the same country, to enable Absa to comply with its legislative requirements.

10 Regulatory Requests	The third party must inform Absa of an event where a regulator requests access to our personal information or initiates an investigation so that we are given an opportunity to respond to such request.	Absa must be notified of regulatory requests so that the appropriate responses are prepared and provided to the applicable requesting regulators to mitigate the risk of non-compliance with any relevant laws and regulations.
11. Third party Assurance	The third party must co-operate where we have a right to audit privacy-related controls upon request.	Absa's right to audit the Supplier's privacy controls is important to ensure that the Third party adheres to Absa's privacy requirements, and not subject Absa information to the risk of information leakages and privacy breaches.