WOOLWORTHS FINANCIAL SERVICES

External Supplier Control Obligations
Data Privacy

Version 7.2 Dated May 2020

Control Title	Control Description	Why this is important
1. Permitted Purpose	Personal data is collected only where permitted by law and for a specified, explicit and legitimate purpose and not processed in a way incompatible with that purpose. The supplier must only process the personal data in line with the obligations of the order/agreement.	Suppliers must follow WFS' instructions so that personal data is only processed for its purposes or else WFS violates laws in most countries where it operates resulting in severe penalties and damage to reputation.
2. Transparency and Openness	Where the supplier is acting as a data controller/responsible party from whom WFS have purchased data/personal data, the supplier must warrant that it has obtained the required consents and/or privacy notice in place to process the data subject's personal data for the purpose for which it is now being processed.	WFS and the supplier must act responsibly and in line with data privacy legislation to ensure that data subjects are informed of or consent to the processing of their personal data, to prevent complaints, penalties and reputational damage.
3. Appropriate Security	The supplier must implement and execute appropriate and sufficient technical and procedural security and organisational controls to prevent personal data from being accidentally or deliberately compromised, damaged or lost.	Suppliers must appropriately protect personal data against accidental or deliberate unauthorised disclosure, misuse or loss to prevent damage to WFS' clients, customers, directors, suppliers and employees, and so that WFS will not violate laws in most countries where it operates
4. Data Accuracy	Records containing personal data must be kept accurate and updated when needed; and identified errors must be corrected	Suppliers must maintain accurate personal data so that WFS can comply with legal requirements in most countries where it operates.
5. Data Relevance and Retention	Personal data collected must be relevant and not excessive in relation to the purpose and must only be retained for as long as necessary. Data must be retained in line with local legislation and securely deleted/de-identified once the data expires/as per agreement.	Suppliers must follow WFS' data collection and retention instructions so that WFS does not violate laws in most countries where it operates.
6. Effective Reporting	Effective mechanisms must be implemented so that potential harm from unauthorised disclosure, misuse or loss of personal data or similar breach are detected, reported, managed and remediated promptly or sooner as agreed. The supplier must inform WFS of a data breach immediately upon discovery of the breach.	The effective and efficient reporting of data breaches to WFS is essential to ensuring appropriate responses and to manage the possible escalation of events to respective regulators.
7. Documented Standards	Annually updated data privacy policies and procedures based on applicable laws are available to demonstrate organisational compliance with these requirements; are linked to proven contractual enforcement mechanisms; and are regularly communicated to all relevant staff. The supplier's policies, processes and procedures align with applicable privacy legislation in all respects with regards to the processing of personal data and should	Updated policies and procedures with detailed individual roles and responsibilities are necessary to determine if Supplier performance meets applicable legislative requirements, and WFS' standards and if Supplier 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 change significantly, they would bring it to WFS' attention as this may require an amendment to the Agreement. The supplier must follow a rigourous HR process prior to employing individuals who deal with personal data. The supplier must follow due process in terms of aligning with applicable privacy legislation to register/notify relevant regulators of their processing activities, as well as obtaining prior authorization, where required.	
8. Privacy Awareness Training	Appropriate Privacy training and material is given to relevant staff to make them aware of data privacy requirements and documented standards.	Training and material are necessary to create Supplier personnel awareness of their individual data processing roles and privacy responsibilities
9. Data Subject Requests and Complaints	The supplier must have processes in place, aligned with applicable legislation, to: – manage challenges raised on the accuracy of data subject personal data, – delete/destroy personal data upon request of the data subject, – manage a data subject's objection to the processing of their personal data – manage the marketing preferences of the data subject (only where relevant) – manage complaints raised by data subjects in the event of their privacy rights being breached The supplier must warrant that where a data subject's rights have been exercised, we are notified of the matter and will respond in accordance with applicable privacy legislation. The supplier must notify WFS in the event that a complaint is raised against WFS so that we are able to respond accordingly.	Replying to or forwarding data subject requests in respect of their personal data and for any other requests or complaints relating to WFS' use of their personal data is necessary to comply with WFS' legal requirements
10. Processing Changes	Personal data processing changes, including country location changes, are notified and agreed before change is implemented. Any further processing of personal data is forbidden unless explicit consent is obtained from WFS to do so.	Prior notification of, and WFS' agreement to, any processing changes is essential to enable WFS to comply with its legal requirements.
11. Sub Processing and Onward transfers	Binding corporate rules or a data transfer agreement must be in place between the supplier and any other entities within their organisation, in the event that personal data is transferred onwards, and those rules/agreements must be aligned to the requirements of this agreement. Where personal data is transferred onward to a sub-processor, WFS must be made aware of this transfer, agree to it and the agreement with the sub-processor must be aligned to WFS' requirements.	Sub processors and onward transfers, whether cross-border or within the same country, must conform with all privacy requirements to enable WFS to comply with its legislative requirements.

12. Regulatory Requests	The supplier must inform WFS of an event where a regulator requests access to our personal data, so that we are given an opportunity to respond to such request.	WFS 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.
13. Supplier Assurance	The supplier must co-operate where we have a right to audit privacy-related controls upon request.	WFS' right to audit the supplier's privacy controls is important to ensure that the supplier adheres to WFS' privacy requirements, and not subject WFS data to the risk of data leakages and privacy breaches.