

External Supplier Control Obligations Data Privacy

Control	Control Description	Why this is important when supplier is acting as a data processor*	Why this is important when supplier is acting as a data controller*
1. Data Collection and Permitted Purpose	Personal data is collected only where permitted by law, individual data subjects are given all of the relevant processing information including a specified, explicit and legitimate purpose; and their personal data is not processed in a way incompatible with that purpose	Suppliers must follow Barclays instructions to ensure that individual data subjects have received all relevant processing information and so that personal data is only processed for the specified purposes or else Barclays violates laws in most countries where it operates resulting in severe penalties and damage to reputation	When collecting personal data suppliers must ensure that individual data subjects have received all relevant processing information so that personal data is only processed for the specified purposes and suppliers comply with laws where it performs for Barclays
2. Appropriate Security	Appropriate measures are implemented so that personal data when stored, processed or transferred is protected against accidental or deliberate unauthorised disclosure, misuse or loss and is securely disposed of as required	Suppliers must appropriately protect personal data against accidental or deliberate unauthorised disclosure, misuse or loss to prevent damage to Barclays customers and employees, and so that Barclays will not violate laws in most countries where it operates	Suppliers must appropriately protect personal data against accidental or deliberate unauthorised disclosure, misuse or loss to prevent damage to individual data subjects including Barclays customers, and employees so that suppliers comply with laws where it performs for Barclays
3. Data Accuracy	Records containing personal data are kept accurate, updated when needed and identified errors are corrected	If in scope of the services, suppliers must maintain accuracy of Barclays personal data so that Barclays can comply with legal requirements in most countries where it operates	If in scope of the services, suppliers must maintain accuracy of Barclays personal data so that suppliers comply with laws where it performs for Barclays
4. Data Relevance and Retention	Personal data is relevant and not excessive in relation to the purpose and is kept only as long as necessary	Suppliers must follow Barclays data collection and retention instructions so that Barclays does not violate laws in most countries where it operates	Suppliers must publish and follow their data collection and retention processes so that suppliers comply with laws where it performs for Barclays
5. Effective Reporting	Effective mechanisms are implemented so that potential or actual harm from unauthorised disclosure, misuse or loss of personal data or similar breach are detected, reported, managed and remediated promptly or as required by law and all of this is documented	Data security relies on a Supplier's timely and effective systems to detect, report, manage and remediate breaches promptly or to comply with specific statutory deadlines such as 72 hours in order for Barclays to comply with its legal requirements for data incident reporting	Data security relies on a Supplier's timely and effective systems to detect, report, manage and remediate breaches promptly to meet specific statutory deadlines such as 72 hours to comply with its legal requirements for data incident reporting
6. Documented Processing and Standards	Regularly updated data processing register documenting processing and identifying high risk processing and data privacy policies and procedures based on applicable law are available to demonstrate organisational compliance with these requirements; are linked to proven contractual enforcement mechanisms; and are regularly communicated to all relevant staff	Updated processing record showing processing activity and high risk processing plus privacy policies and procedures with detailed individual roles and responsibilities must show that Supplier is complying with Barclays standards; is regularly communicating these to staff and is enforcing them against staff who must comply with contractual confidentiality and privacy obligations during and after their employment	Updated processing record showing processing activity and high risk processing plus privacy policies and procedures with detailed individual roles and responsibilities must show that Supplier complies with laws and/or best practices; is regularly communicating these to staff and is enforcing them against staff who must comply with contractual confidentiality and privacy obligations during and after their employment

7. Privacy Awareness Training	Appropriate Privacy training and material is given to relevant staff to make them aware of data privacy requirements and documented standards	Records of regular Supplier staff training and a copy of training material are necessary to demonstrate Supplier staff awareness of their individual data processing roles and data privacy responsibilities	Records of regular Supplier staff training and a copy of training material are necessary to demonstrate Supplier complies with laws and/or best practices relating to staff awareness of their individual data processing roles and data privacy responsibilities
8. Data Subject Requests	Requests from individuals identifiable from personal data are notified and/or forwarded without undue delay so that they can be acted upon to enable compliance with applicable law	Replying to or forwarding data subject requests for data portability or to access, correct, erase, restrict or object to the processing of their personal data and for any other requests or complaints relating to Barclays use of their personal data without undue delay is necessary to comply with Barclays legal requirements	Replying to or forwarding data subject requests for data portability or to access, correct, erase, restrict or object to the processing of their personal data and for any other requests or complaints from Barclays customers or employees without undue delay is necessary to comply with suppliers legal requirements
9. Processing Changes	Personal data processing changes, including country location changes, apply privacy by design and are supported by data privacy impact assessments and notified and either agreed by Barclays or accepted by data subjects as applicable before change is implemented	Prior notification of, and Barclays agreement to, any processing changes supported by data privacy impact assessments is essential to enable Barclays to comply with its legal requirements	Prior notification and acceptance of any processing changes supported by data privacy impact assessments is essential to enable supplier to comply with its legal requirements
10. Sub Processing	Proposed sub processors of personal data are agreed in advance and subject to appropriate written subcontracts	Sub processors must be selected for their ability to conform with all privacy requirements and, after Barclays approves, their contracts must have appropriate provisions, including Data Transfer Agreements	Sub processors must be selected for their ability to conform with all privacy requirements and their contracts must have appropriate provisions, including Data Transfer Agreements

*A data processor will process personal data on behalf of Barclays. It will follow Barclays data processing instructions and implement appropriate security measures agreed by Barclays. A data controller (or owner) determines the means and purposes of processing personal data. It will process personal data of Barclays customers or employees with whom it has contracted. It will typically but not always be a regulated entity or will be performing regulated services.