LLOYDS BANKING GROUP	**GROUP DATA PRIVACY POLICY** **SUMMARY FOR THIRD PARTY SUPPLIERS**

RATIONALE

Lloyds Banking Group (the Group) has a moral, legal and regulatory responsibility to protect the privacy of individuals who provide us with personal information. This extends to activities carried out for or on behalf of the Group by its Third Party Suppliers.

This Policy defines the Group's requirements that its suppliers must meet to ensure a robust and consistent approach to the management of data privacy thereby mitigating the risk of regulatory censure, litigation and loss of stakeholder confidence. These requirements are informed by the:

- Directive EC/95/46/EC Data Protection
- Directive 2002/58/EC Privacy and Electronic Communications
- Data Protection Act 1998 (UK)
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (UK)

The Group's vision is to be the best bank for customers. The Data Privacy Policy supports this vision by:

- Enabling the business to process personal information in line with legal/regulatory expectations to deliver sustainable growth and become simpler and more efficient;
- Clearly communicating to customers how their personal information will be used and disclosed, ensuring such use is in line with their expectations;
- Holding and using customer personal information securely; and
- Enabling customers to exercise their Rights, as set out in data privacy legislation.

SCOPE

This third party version of the Data Privacy Policy applies to any supplier that provides goods or services that involve the handling of personal information, and may be impacted by data privacy risks.

Personal information is defined as any information that can be used, either on its own or with other readily available information to identify a living individual, for example, a customer or colleague.

MANDATORY REQUIREMENTS – GENERAL

Roles and Responsibilities

All Third Party Suppliers must ensure:

- Personal information processing is compliant with the requirements as set out in the contract between the third party supplier and the Group.
- A nominated data privacy contact and sufficient resource is in place with the

necessary skills and knowledge developed and maintained to discharge data privacy accountability under the contract.
- Risk based monitoring plans are established and embedded.
- Data privacy risks, incidents or Policy breaches are identified and reported to the Group to action appropriate remediation and regulator engagement.
- Process or procedure changes are assessed to understand any data privacy impact.
- The data controller and data processor requirements are understood, agreed and documented.

Privacy Management

Fair and Lawful Processing

- Only collect personal information as specified by the Group in order to provide the contracted products / services and where necessary, obtain the individual's consent.
- Through a compliant data privacy notice (provided by the Group where applicable), inform all individuals about how their personal information will be used. An audit trail of data privacy notices must be used and maintained.
- Personal information should only be processed for the specified purposes for which it has lawfully been collected.

Data Quality

- Ensure personal information held is accurate and, where necessary, kept up-to-date.
- Delete or destroy personal information in line with the requirements of the 'Destruction' section of the Records Management Policy Summary for Third Party Suppliers.
- Ensure that adequate, relevant but not excessive personal information is collected to fulfil the activities specified in the contract with the Group.

Respecting Individuals' Rights

In line with contractual obligations:

- Manage individuals' requests to access their personal information (e.g. data subject access request or 'DSAR'), including providing the information the individual is entitled to.
- Manage individuals' marketing preferences across all communication mediums (e.g. mail, phone, email, SMS and online).
- Respond to requests to prevent or review automated decisions, to change or amend personal information, or to cease processing that is causing damage or distress.

Security of Personal Information:

Personal information must be protected against accidental or deliberate misuse, damage or destruction, ensuring:

- Suppliers comply with the requirements of the Group Information & Cyber Security Policy Summary for Third Party Suppliers.
- Sub-processors are subject to due diligence and contracts reflect the

equivalent requirements between the Supplier and the Group; Disclosures of personal information are undertaken in compliance with the law, including maintenance of records to identify disclosures of personal information to third parties such as police, government bodies etc. with a clear rationale as to why the disclosure was valid.

- Any access to personal information is only where there is a valid business or legal/regulatory need to do so.
- In line with the Minimum Information Handling Requirements, particular care is given to personal information, both paper and electronic formats, when removed from Supplier premises.

Transferring Personal Information to Another Jurisdiction

Personal information processed in the European Union (EU) must not be transferred to countries outside the European Economic Area (EEA) unless approved by the Policy Owner. All contracts with Suppliers based outside the EEA must contain the EU Model Contract Clauses, unless the country is deemed as 'adequate' by the EU (See list of countries with 'adequacy' here).

Risk, Compliance and Governance

- Ensure as a minimum the Data Privacy Policy and supporting Procedures are embedded and ongoing control testing plans are in place to monitor compliance with policy and identify emerging risks.
- Ensure that data privacy requirements are considered at the start of any change management activity. An assessment of the privacy and records management impact must be completed.

Employee Training

The Supplier's employees must be appropriately trained, including during induction, to understand how the requirements of this Policy affect their role and their responsibilities for compliance.

KEY CONTROLS

The following indicators must be monitored and reported on by the business to evidence operating effectiveness of the mandatory key controls.

Control Title	Control Description	Frequency
1. Privacy contact and appropriate resource is in place to discharge privacy accountabilities.	Privacy contact is appointed. GREEN =Yes RED = No	Quarterly
2. Timely completion of Data Subject Access Requests and Requests for Personal Information to allow the Group to complete a DSAR in a compliant manner	% breach of legal timescale: GREEN = 0.49% or below issued later than legal timescale AMBER = 0.50 - 0.54% issued later than legal timescale RED = 0.55% or above issued later than legal	Monthly

	timescale	
3 Privacy impact assessment (PIA) of proposed changes at the planning stage of all change projects to ensure any privacy risk mitigation is built in. PIA included in change management process.	PIAs completed for change management projects. GREEN = 100% RED = 99% or below -	Quarterly
4. Sub-processor contracts reflect equivalent requirements. Supplier to provide attestation that they have completed due diligence on sub-processors relied upon to deliver services to the Group; and equivalent controls are reflected in Supplier/sub-processor contracts.	Due diligence completed. GREEN = 100% RED = 99% or below Equivalent contractual controls in place with sub-processors. GREEN =100% RED = 99% or below -	Quarterly

MANDATORY REQUIREMENTS – NON-COMPLIANCE
Any material differences between the requirements set out above and the supplier's own controls should be raised by the Supplier with Lloyds Banking Group's Supplier Manager. The Supplier Manager will then discuss the non compliance with the Accountable Executive for the relationship and BUCF to agree way forward.

Version Number	Effective Date
1.0	May 2014
2.0	15 January 2015
3.0	17 December 2015
Next Planned Revision: October 2016	

Further information: Information Commissioner's Guidance on Model Contract Clauses

https://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/model_contract_clauses_international_transfers_of_personal_data.ashx