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

RATIONALE

The Group Data Policy has been designed to assist in managing the risk of Lloyds Banking Group ('the Group') ***failing to effectively govern, manage, and protect its data throughout its lifecycle, including data processed by third party suppliers, or failure to drive value from data; leading to unethical decision making, poor customer outcomes, loss of value to the Group and mistrust.***

This Policy has been designed to specifically support compliance with the following legislation and / or regulations:

- General Data Protection Regulation (EU) 2016/679, Data Protection Act 2018, and Directive 2002/58/EC, UK GDPR 2021, Privacy and Electronic Communications (in relation to the requirement for consent) and prevailing jurisdictional and other amendments
- Basel Committee on Banking Supervision ("BCBS") Principles for effective risk data aggregation and risk reporting (BCBS239)
- FCA Senior Management Arrangements, Systems & Controls, SYSC 9.1 General Rules on record keeping

This policy also supports compliance with any specific record keeping and data management related requirements contained in other laws and regulations that rely on data being assured and accurate.

The following **PRINCIPLES** clarify the outcomes which are intended to be achieved through the Group's compliance with its Data Policy.

PRINCIPLE	***RISK MITIGATED***
Principle 1 - *Data Governance* *We have robust processes and accountabilities in place to demonstrate we are doing the right thing with data.*	Risk of the Group failing to effectively **govern** and provide robust oversight of data decision making and control mechanisms
Principle 2 - *Applied Data Management* *We are committed to avoiding detriment to our customers, colleagues and others, as a result of our data practices. We will conscientiously provide and consume relevant data to facilitate good customer, colleague and regulatory outcomes.*	Risk of the Group failing to effectively **manage** its data (or the data shared with Third Party Suppliers) impacting quality, retention, traceability and **understanding** of data and records.
Principle 3 - *Data Quality* *All data in LBG should be fit for purpose and fulfil a given business requirement, customer*	

data is especially important to us; we will "put it right when it goes wrong".	
Principle 4 - *Data Traceability* *We will document where data is sourced from, where it is held, what it means and how it flows.*	Risk of the Group failing to effectively **manage** its data (or the data shared with Third Party Suppliers) impacting quality, retention, traceability and **understanding** of data and records.
Principle 5 – *Data Retention & Retrieval* *We will create and maintain records of our business activities, retrieving, retaining and disposing of them in line with legal, regulatory and internal requirements.*	
Principle 6 - *Data Privacy* *We value the trust our customers and colleagues place in us, and will always process their Personal Data in a lawful, fair and transparent manner.*	Risk of the Group failing to acquire or **process** data **ethically,** legally**,** for a legitimate purpose, or is not managed/protected from misuse and/or processed in a way that is transparent and complies with data protection regulations.
Principle 7 - *Data Ethics* *We will ensure ethical data processing and design, leading to fair, explainable and non-discriminative outcomes.*	

It is expected that Group suppliers will acknowledge these principles and endeavour to provide their products and services in a manner that supports and enables the Group to uphold them.

SCOPE

This third party version of the Data Policy applies to any supplier that:

1. provides goods or services that involve the processing of *personal data*, and may therefore be impacted by data privacy risks;
2. create, store, process, retain, retrieve, access or dispose of the *Group's records* or may be impacted by records management risks;

It primarily addresses the legal obligations associated with data protection legislation and also the legal and regulatory requirements to maintain records of the Group's business activities. Scope and mandatory requirements for suppliers fall into three categories.

Personal Data Processing (mandatory requirements Section 1)

This Policy applies to all personal data regardless of media, including paper and electronic formats, under the controllership of Group legal entities. All references to personal data throughout this Policy Summary include special categories of personal data, unless specifically stated.

Records and Managing Records (mandatory requirements Section 2)

A record is evidence of an event and due to legal, regulatory and /or business requirements should be retained. Records enable the Group to manage our conduct risk and continue to evidence our fair, lawful, and ethical customer interactions. They can be distinguished from other types of information by their role as evidence of business activity and by the fact that they have context which we need to preserve. For example, contracts, financial statements, customer correspondence, colleague

pay and awards and compliance arrangements. Records can be structured in a system or unstructured in other platforms such as SharePoint, Outlook, shared drives, and can also be physical e.g. paper, microfilm. Records can include personal data and special categories of personal data, and for these the requirements of Section 1 also apply.

Data Management (mandatory requirements Section 3)

Suppliers who process Group data as per sections 1 & 2 must document where data is sourced from, where it is held, where it is transferred, processed, ingested and consumed. Suppliers must also have methods in place to ensure the ongoing quality of data processed for or on behalf of the Group.

Suppliers operating outside the UK must ensure that local country and jurisdictional legislation and/or requirements are adopted in addition to the requirements of this Policy. Local laws or regulations (e.g. maximum retention periods) may take precedence over or be in conflict with this policy, in these circumstances exceptions and equivalence must be agreed with the Group's Supplier Manager.

Where suppliers are using their own third parties (also referred to as the Group's 4th parties) to fulfil part of contracted services, the Supplier to the Group must ensure that the standards operated by the Group's 4th party are of an equal level to those operated by the Group.

MANDATORY REQUIREMENTS – GENERAL

Section 1 – Personal Data Processing

Roles and Responsibilities

The supplier must ensure:

- personal data processed on behalf of the Group is compliant with GDPR and the requirements set out in the contract between the supplier and the Group;
- a nominated data privacy contact and sufficient resource is in place, with the necessary skills and knowledge to discharge data privacy accountability under the contract;
- risk based monitoring plans are established and embedded.

Privacy Management

- **Personal data is processed lawfully, fairly and transparently.**

The supplier must:

- where the supplier is responsible for providing DPNs under the terms of their agreement with LBG, suppliers must inform an individual about how their

personal data will be used and their individual rights by using an approved Group data privacy notice ("DPN"), including cookie notices;

- where personal data has not been obtained from an individual, provide the individual with a suitable data privacy notice within a reasonable period, and at least within one month, unless Data Privacy law does not require us to do so;
- ensure that DPNs are easily accessible, not included within the general contractual terms and conditions, only include information relevant to the data capture and are provided free of charge.

- **Personal data is collected for specified, explicit and legitimate purposes and not further processed in ways that are incompatible with those purposes.**

The supplier must not process personal data contrary to its original purpose or otherwise outside an individual's expectations.

Records of Processing Activity

The supplier must:

- maintain evidential Records of Processing Activity undertaken on behalf of the Group, as a Data Processor in line with Article 30 (Section 2, 3, 4 and 5) of the General Data Protection Regulation (GDPR);
- in consultation with the Group's Data Privacy Officer (GDPO), make the Records of Processing Activity available to relevant Supervisory Authorities on request.

Data Privacy Impact Assessments

The supplier must complete an appropriate risk assessment at the start of (and review during the lifecycle of) all change activity involving the Group's personal data in order to identify, assess, manage and evidence data privacy risks, including:

- details of the envisaged processing operations;
- purpose of the processing and, where applicable, the legitimate interest pursued;
- necessity and proportionality of the processing;
- if the processing is High Risk;
- risks to the right and freedoms of data subjects;
- required measures to address the risks (privacy by design and default).

In consultation with the Group's Supplier Manager, consider whether it is appropriate to seek the views of individuals or their representatives on the intended processing.

The supplier must review previously completed Data Privacy Impact Assessments when there is a change to the risk represented by processing operations.

Upon request, suppliers will provide the Group with any information about the processing of Lloyds Banking Group data which is necessary to support our completion of Data Privacy Impact Assessments or other similar risk assessments.

Consent Management and Direct Marketing

Where the supplier contract stipulates that the supplier manages consents and/or direct marketing on behalf of the Group, the supplier must:

- ensure they can manage, record and evidence consent, including consents in relation to special categories of personal data, children and vulnerable

customers, provided in relation to the collection or processing of personal data, and manage and record any change or revocation of consent;

- ensure that consent to processing (including marketing permissions) can be easily withdrawn at any time, upon request;
- be able to manage marketing permissions across all communication channels (e.g. mail, phone, email, SMS/text, device messaging and internet banking) during initial data collection.

- **Personal data is adequate, relevant and limited to what is required.**

The supplier must ensure the personal data it processes on behalf of the Group is adequate, relevant and not excessive in relation to the purposes for which it is processed.

- **Personal data is accurate and, where necessary, kept up to date, and will amend or delete inaccurate personal data without delay.**

Where the supplier is contractually required to take steps to amend/delete inaccurate data they must:

- ensure personal data is kept accurate and up-to-date;
- take every reasonable step to ensure inaccurate personal data is securely deleted or amended without delay, after agreement with the Group if necessary;
- communicate any rectification to or erasure of personal data to any recipients (e.g. Credit Reference Agencies) to whom the personal data has been disclosed.

- **Personal data will be retained for as long as it is required to support our business processes.**

The supplier must:

- keep personal data in a form that permits identification of Data Subjects for no longer than is necessary, in line with the requirements set out in Section 2 of this document.
- ensure any deletion of personal data which is no longer required is completed securely, in line with the requirements set out in the Minimum Security Standards Third Party Policy.

- **Appropriate technical and organisational measures will be adopted to ensure personal data is processed securely.**

The supplier must ensure personal data is protected against unauthorised or unlawful processing and against accidental loss, destruction or damage in accordance with the Minimum Security Standards Third Party Policy and in particular relating to:

- the pseudonymisation and encryption of personal data;
- the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore availability and access to personal data in the event of a physical or technical incident;
- regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

The supplier must not appoint a sub-contractor to process Group personal data without the Group's prior specific or general written authorisation. All sub-contractors must be subject to due diligence and contracts must reflect the equivalent requirements between the supplier and the Group.

Management and Reporting of Personal Data Incidents / Breaches

The supplier must:

- Report personal data incidents / breaches to the Group, via the Group's Supplier Manager, as soon as they become aware of them and no more than 24 hours after identification or in line with agreed contractual obligations.
- Assist the Group in documenting personal data incidents / breaches, comprising the facts, its effects and the remedial actions taken.
- Where a personal data incident / breach is likely to result in a risk to the rights and freedoms of natural persons, assist the Group, as necessary, in reporting the breach to the relevant Supervisory Authority.
- Keep records of personal data incidents / breaches, comprising the facts, its effects and the remedial action taken.

Requests for Disclosure of Personal Data

The supplier must ensure requests for disclosures of personal data from Regulators, Government, Local Authorities and/or Law Enforcement agencies are:

- Authenticated - to establish the requestor is who they say they are;
- Validated – to confirm the requestor is entitled to all of the information being requested;
- Responded to securely and in accordance with the Minimum Information Handling requirements set out in the Minimum Security Standards Third Party Policy; and
- Retained in line with requirements in Section 2 of this document, and in particular that an audit trail is maintained which includes a clear explanation as to the rationale for disclosure.

Colleague Training

The supplier must ensure all employees/contractors complete Data Privacy training within eight weeks of commencing employment and annually thereafter to understand how the requirements of relevant data privacy legislation and this Policy Summary affect their role and individual responsibilities.

- **Rights individuals are provided with under data privacy laws will be respected and complied with.**

Data Subject Access Requests (DSARs)

In line with contractual obligations the supplier must manage individuals' requests to access their personal information (i.e. data subject access request or 'DSAR'); including providing the information the individual is entitled to.

When providing the Group with personal data to respond to a DSAR request, the supplier must not alter, deface, block, erase, destroy or conceal the disclosure of personal data which the individual making the request would have been entitled to receive. The Group reserves the right to report suppliers found guilty of committing such an offence to the relevant Supervisory Authorities who may consider criminal prosecution.

Data Privacy Complaints

The supplier must ensure complaints received from Supervisory Authorities and non-profit bodies, organisations or associations, whose statutory objectives are in the public

interest, are forwarded to the Group's Supplier Manager without delay and no more than 24 hours after receipt or in line with agreed contractual obligations.

The supplier must assist the Group, as necessary, in investigating and drafting any response to data privacy complaints received from Supervisory Authorities and non-profit bodies, organisations or associations, whose statutory objectives are in the public interest.

Other Data Privacy Rights

The supplier must have processes in place to respond to requests to:

- rectify inaccurate personal data without undue delay;
- erase personal data ('right to be forgotten');
- restrict processing;
- transfer personal data to another legal entity ('right to data portability'), for example a competitor bank, in a structured, commonly used and machine-readable format;
- object to processing;
- prevent or review decisions, including profiling, based solely on automated processing.

The supplier must ensure they communicate any rectification, erasure or restriction of processing of personal data to each recipient to whom personal data has been disclosed, except where such communication is impossible or involves disproportionate effort.

The supplier must escalate, without delay and no more than 24 hours after receipt, or in line with agreed contractual obligations, any requests they cannot complete as part of business as usual processes to the Group's Supplier Manager or direct to the Group's Data Privacy & Records Management Team.

- **Personal Data will only be transferred to third countries or international organisations where adequate measures exist to enable the transfer to take place.**

Suppliers must not process personal data in any geographical jurisdictions other than those agreed with contractual documentation without first obtaining agreement from the Group.

The supplier must ensure personal data processed in the United Kingdom ("UK") and the European Economic Area ("EEA") is not transferred to countries outside the UK and EEA (see list of countries inside the EEA here) unless:

- the country to which the personal data is being transferred is considered to have adequate protection in place, by either the UK or European Commission (see list of countries with UK 'adequacy' here and EU adequacy here);
- the transfer has appropriate safeguards in place (e.g. Binding Corporate Rules, EU or UK Standard Contractual Clauses (SCCs), an approved code of conduct etc.); or one of the limited derogations set out in Article 49 of the GDPR apply.

Section 2 – Records & Managing Records

Different suppliers provide different services to the Group and therefore have different responsibilities for the Group's Records.

Therefore this Policy may be relevant in part or in whole to suppliers depending on the services they provide, as set out in the contract between the supplier and the Group.

The following requirements apply if a supplier undertakes one or more of the following; create, store, process, retain, retrieve, access or dispose of the Group's records.

Accountability

Suppliers must ensure that:

- They appoint a person, in accordance with the supplier's governance structure, to be accountable for the effective management of the Group's records in line with this policy, monitoring the key controls defined below and for confirming to the Group's Supplier Manager that the Records Management capability meets the Group's requirements.
- They have a Records Management framework in place which ensures compliance with legislation, regulation and this Policy (as appropriate).
- They have ongoing control testing/assurance plans and adequate governance in place to monitor compliance with Policy, identifying where remediation is required and implementing agreed actions.
- Records Management requirements are considered if there is any change to their business processes or location that could impact the creation, management, storage, retention, preservation or disposal of Group records. The Group must be notified of any impacts.
- Upon exit the supplier, in agreement with the Group, must return or dispose of Group Records.
- Records management risks, incidents or events are identified and reported to the Group's Supplier Manager.
- Group's Records shared with them are protected and are disposed of on the request of the Group
- The supplier's employees are appropriately trained to understand how the requirements of this Policy affect their role and their responsibilities.

The supplier must identify and maintain (reviewed using a trigger based approach or annually as a minimum) a list of the Group's Records that it creates, stores, processes, retains and disposes. The list should include as a minimum, the type of record, where it is stored, retention period and if it is subject to a retention hold.

The Group's records must be created and maintained so that they are:

- Accurate and complete: Records must contain all the information that is expected or required to be in the record.
- Reliable: Record content must be trusted as an accurate representation of the activities or facts to which they attest.
- Usable: Records, Personal Data and Special Categories of Personal Data must be legible and able to be interpreted throughout their life.

The Group's records must be able to be located and retrieved when requested and within the timescales stipulated.

The Group's records must be stored in a location that ensures the record will remain accurate, authentic, legible and retrievable.

Group Data Policy Summary For Third party Suppliers

Suppliers are required to agree retention periods with the Group as part of contractual agreements. Notwithstanding any overriding legal and / or regulatory requirements to retain certain records for a shorter or longer period, the Group's Records must be retained for no longer than necessary and in accordance with the rules below:

Retention Period:	Applicable to:
Dispose After Use	If it is not a Record, or if it is a Record where there is no legal or regulatory reason to retain after business use, e.g. unfulfilled customer application, forms must be disposed of after business use. The period of retention would not typically exceed 36 months
7 Years	Records can be retained for a maximum of 7 years from a predefined trigger event. 7 years reflects statutory liability of 6 years, plus 1 additional year to complete the data processing lifecycles e.g. record disposal
10 Years	If there is a legal or regulatory reason to retain Records beyond the 7 years, a maximum of 10 years from a predefined trigger event* can be utilised but must be approved with the Group. The rationale for retaining Records beyond 7 years must be documented in the list of Group's Records and subject to annual Group approval. *Note: If 10 years is the current agreed retention of the Groups Records by the supplier, it is acceptable for the retention period to be reviewed as part of the next contract review.*

*A trigger event is the event that instigates the start of the retention period e.g. account closure.

Retention periods can be overridden for legal or regulatory investigation purposes. Records pertaining to a pending or actual litigation, legal action or investigation must not be disposed. Suppliers must ensure they can apply and release retention holds to the Group's records as and when preservation notices are issued by the Group.

Group's records with historical or long-term business value must be sent or made available to the Group to enable them to be considered for permanent retention by Group Archives.

Group's records must be protected and secured throughout their lifetime. Controls must be in place to prevent unauthorised access, alteration, concealment or disposal.

Controls must be in place to identify the Group's time-expired Records (i.e. records that have reached the end of their retention period) and must be securely disposed of at the end of the agreed retention period.

All disposals must be authorised and evidenced to LBG, this includes the authorisation and the evidence of the authorisation and disposal.

Section 3 – Data Management

Suppliers who process Lloyds Banking Group data per sections 1 & 2 must document where data is sourced from, where it is held, where it is transferred, processed, ingested and consumed. The Supplier must ensure they hold and follow good data management practices throughout the data lifecycle, and methods are in place to ensure the ongoing quality of data processed for or on behalf of the Group. As a minimum requirement we would expect that;

- Suppliers have and maintain a data quality policy, procedure or principal document
- Data quality is controlled throughout the lifecycle of data (including capture / creation, storage, change, maintenance, disclosure & use)
- Data quality requirements should be clearly defined, with measurement, monitoring and reporting of data quality communicated to the Group
- Data quality failures are recorded and communicated to the Group without delay
- A process or procedure to manage data quality issues such as the timely escalation and / or engagement model for data quality issues identified within the receipt, processing, retrieval and deletion of the Group's Data
- Suppliers have ongoing control testing/assurance plans and adequate governance in place to monitor compliance with this Policy, identifying where remediation is required and implementing agreed actions

Suppliers have and maintain a Metadata Management Policy, procedure or principal document. The contents of that document should include:

- A process to catalogue the metadata for any data being processed
- A process to document the data lineage associated with any data being processed, including clear explanation of any data transformations
- A process to ensure data is classified accurately, this may include the categories of personal data or a security classification (i.e. Public vs. Confidential)

Group Data Policy Summary For Third party Suppliers

KEY CONTROLS		
Control Title	**Control Description**	**Frequency**
Contractual Documentation	Where the supplier is using a sub-processor outside of the UK and the EEA to process LBG data, the supplier can evidence that appropriate UK or EU Standard Contractual Clauses, or another valid mechanism of transfer, are in place.	Annually
Accountability for Data Privacy Compliance	The supplier can evidence that a nominated individual has been appointed and sufficient resource is in place, with the necessary skills and knowledge, to discharge data privacy accountability under the contract.	Annually
Records of Processing Activity	The supplier can evidence they maintain Records of Processing Activity undertaken on behalf of the Group, as a Data Processor, in line with Article 30 (2, 3, 4 and 5) of the GDPR.	Annually
Management of Sub-contractors who have access to Group personal data	The supplier can evidence they obtained the Group's written permission to appoint sub-contractors who access Group personal data. The supplier can evidence that due diligence was completed at the beginning of and during the lifetime of the relationship with sub-contractors and issues identified during reviews have been/are being actioned/remediated. The supplier can evidence that equivalent contractual controls are in place with sub-processors.	Annually
Data Privacy Colleague Training	The supplier can show evidence that all supplier employees who have access to Group personal data have completed mandatory Data Privacy training within 8 weeks of commencing employment with the supplier and annually thereafter.	Annually

Group Data Policy Summary For Third party Suppliers

List of Group Records	The supplier can show evidence of how they have identified and maintained a list of the Group's Records that it creates, stores, processes, retains and disposes. The supplier can show evidence that it has maintained and quality reviewed the list using a trigger based (e.g. a new record is created, or a record retention period for an existing record changes) approach or annually as a minimum.	Annually
Creation and Retrieval	The supplier can show evidence that the Groups Records are accurate and complete, reliable and usable and can be located and retrieved when requested. A sample of Records are retrieved and checked for a) Accuracy & completeness b) Reliability c) Usability d) Retrieval timeliness	Semi-Annually
Retention & Disposal	Group Records are retained for a period of time in line with the rules in this Policy and disposed of in a timely manner in line with the requirements of this Policy. A sample of the Group's Records is requested and the supplier can show evidence of how it applies the correct retention periods and trigger events to the Group Records. The supplier can evidence that they have controls in place to identify time-expired records, and that disposal is authorised by the Group and is evidenced.	Semi-Annually
Retention Holds	The supplier must be able to preserve Group Records upon request. The supplier can show evidence of how it applies retention holds/preservation notices issued by the Group. E.g. a procedure document and example of how this has been actioned (if applicable)	Annually

Data Quality Management	The Supplier can evidence or describe data quality measurement is conducted to understand the current state of data quality for a given data set. *Two common (but not exhaustive) methods for measuring data quality are:* *Data Profiling: A form of statistical analysis used to validate or discover the true structure, content, and quality of a dataset.* *Data Quality Rules/reporting: When there is a clear understanding of the data standards a piece of data should comply to, a set of data quality rules can be designed with logic to test conformance with those standards. Data quality rules will typically have a threshold of acceptance, once breached the rule will then fail, which could trigger some investigatory action.*	Annually
Data Management	Ensure that Lloyds Banking Group data processed is documented, describing the characteristics and meaning of the data. The Supplier can evidence or describe data dictionary and lineage is documented in a way that describes the business and technical characteristics of data. *Business metadata typically describes the meaning, classification, purpose, value, context, relationships to other data and provenance of data.* *Technical metadata typically describes structure, format, physical representation and instances of data*	Annually

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 the Group's Supplier Manager.

The Group's Supplier Manager will then discuss the non-compliance with the Accountable Executive for the relationship and local Risk team to agree the way forward.

Group Data Policy Summary For Third party Suppliers

Version Number	Effective Date
Version 2.0	26/01/2023
Version 1.0 (superseding previous Records Management Policy Summary V6.0 Final and Data Privacy Policy Summary V5.0	27/04/2020