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

RATIONALE

This Policy has been designed to assist in managing the risk that Lloyds Banking Group ('the Group') ***failing to effectively govern, manage, and control its data (including data processed by Third Party Suppliers) leading to unethical decisions, 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 Privacy and Electronic Communications (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.

Additionally, this policy also supports compliance with any specific record keeping, data assurance and data quality related requirements contained in other laws and regulations.

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, where it is held, what it means and how it flows*	
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 create an ethics framework for processing and managing data to ensure responsible innovation that leads to fair, open 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 or destroy the *Group's records* or may be impacted by records management risks.

It primarily addresses the legal obligations associated with the general data protection laws and also the legal and regulatory requirements to maintain records of the Group's business activities. Scope and mandatory requirements for suppliers fall into these two 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)

Records capture information and provide authoritative evidence about the Group's business activity. 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, campaign briefs, and

compliance arrangements. Records can include personal data and special categories of personal data, and for these the requirements of Section 1 also apply.

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

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

The supplier 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 have 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.

2. **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, and in particular should record:

- 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.

In consultation with the 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.

Consent Management and Direct Marketing

The supplier must ensure they can manage, record and evidence consents, 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.

The supplier must ensure that consent to processing (including marketing permissions) can be easily withdrawn at any time, upon request.

The supplier must 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.

3. **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.

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

The supplier 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.
- 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.

5. Personal data will be retained for as long as they are 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 Group Information & Cyber Security Policy Summary for Third Party Suppliers.

6. 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 Group Information & Cyber Security Policy Summary for Third Party Suppliers and in particular should consider:

- 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 Supplier Manager or direct to the GDPO, 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 Group Information & Cyber Security Policy Summary for Third Party Suppliers; 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.

7. 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 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 Supplier Manager or direct to the Group's Data Privacy & Records Management Team.

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

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

- the European Commission has determined the country to which the personal data is being transferred is considered to have adequate protection in place (see list of countries with 'adequacy' here);
- the transfer has appropriate safeguards in place (e.g. Binding Corporate Rules, EU Model Clauses, 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 a guide, the following categories have been created and they are referenced throughout the Policy where we think they are applicable.

Category A – The supplier creates, manages, stores, preserves and destroys the Group's Record on our behalf at their own premises.

Category B – The supplier manages and stores the Group's Records and/or Personal Data and Special Categories of Personal Data on our behalf at their own premises.

Category C - The supplier destroys only (not stores) the Group's Records and/or Personal Data and Special Categories of Personal Data on our behalf at their own premises.

Category D – The supplier processes the Group's Records and/or Personal Data and Special Categories of Personal Data on our behalf at their own premises but does not store or retain any copies.

Category E - The supplier processes the Group's Records and/or Personal Data and Special Categories of Personal Data on our behalf at/on systems at the Group's premises.

Category F – The supplier does not create or have any access to the Group's Records and/or Personal Data and Special Categories of Personal Data.

Accountability (Applicable to supplier categories A, B, C, D, E)

Suppliers must ensure that:

- They appoint a person, in accordance with the supplier's governance structure, to be accountable for implementation of 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 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, preservation or disposal of Group records.
- Records management risks, incidents or events are identified and reported to the Group's Supplier Manager.
- Records released to them are protected and that records 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 contract between the third party supplier and Lloyds Banking Group contains the relevant records management clauses detailed in the Group Security Schedule.

The supplier must identify and maintain (review at least annually) a list of the Group's Records that it creates, store, processes, retains or destroys. (Applicable to supplier categories A, B, C, D)

Records, Personal Data and Special Categories must be created and maintained so that they are: (Applicable to supplier categories A, B)

- 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.

Records, Personal Data and Special Categories must be able to be located and retrieved within 10 working days. (Applicable to supplier categories A, B, D)

Storage of Records, Personal Data and Special Categories must be fit for purpose to ensure throughout their lifetime they can be accessed, retrieved and are still legible. (Applicable to supplier categories A, B)

The Group's Records must be retained for as long as is necessary and in accordance with the following rules (Applicable to supplier categories A, B)

Records, Personal Data and Special Categories must be retained for no longer than necessary and in accordance with the rules below: (Applicable to supplier categories A, B)

Record Category:	Retention Period:	Applicable to:
Records containing Personal Data	10 Years	**Records containing personal data and/or special categories of personal data** must be retained for **10 years** from a pre-defined trigger event unless there is a legitimate basis to retain for longer (i.e. actual or risk of legal, regulatory or mandatory hold)
	Dispose After Use	**Records containing personal data and or special categories of personal data** where there is **no legitimate basis** to retain after business

		use, e.g. unfulfilled customer application, forms must be **disposed of after business use**. The period of business would not typically exceed 36 months.
Records not containing Personal Data	Variable – *Business dependent*	The retention of **Records not containing personal data should be defined locally, considering business requirements** in line with legal, accountability or reference purposes.

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, Personal Data or Special Categories of Personal Data pertaining to a pending or actual litigation, legal action or investigation must not be disposed. They must be managed in accordance with the Group Legal Hold Process and local processes. (Applicable to supplier categories A, B, C, D)

Records with historical or long-term business value must be sent or made available to Group Archives and considered for permanent retention. (Applicable to supplier categories A, B)

The above retention periods apply to Records, Personal Data and Special Categories of Personal Data created on or after 22nd April 2013. All records created prior to this date have the option to be are governed by:

- Previous Group Retention Schedules and previous Data Privacy Policies, or
- Take a risk based approach by applying the current retention schedule. This approach must be agreed by the appropriate Group Accountable Person and the Policy Owner

Where there is specific legislation or a regulatory requirement mandating a maximum retention period outside the Group's internal retention categories, the legislation or regulatory requirement must be followed. In this scenario the Group must be informed and approve the exception. (Applicable to supplier categories A, B, C, D)

Records, Personal Data and Special Categories of Personal Data must be protected and secured throughout their lifetime. Controls must be in place to prevent unauthorised access, alteration, concealment or disposal. (Applicable to supplier categories A, B, C, D)

Controls must be in place to identify time-expired Records, Personal Data and Special Categories of Personal Data (i.e. records and/or that reach the end of their retention period). (Applicable to supplier categories A, B, C)

Records, Personal Data and Special Categories of Personal Data must be securely disposed of at the end of the agreed retention period (Applicable to supplier categories A, B, C)

Electronic Records, Personal Data and Special Categories of Personal Data retained within third party structured systems must be securely disposed of in line with the

Electronic Records Procedure at the end of the agreed retention period. (Applicable to supplier categories A, B, C) All disposals must be authorised and evidenced (Applicable to supplier categories A, B, C)

Group Data Policy Summary For Third party Suppliers

KEY CONTROLS		
Control Title	**Control Description**	**Frequency**
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. GREEN =Yes RED = No	Quarterly
Records of Data 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. GREEN = Yes RED = No	Quarterly
Privacy Impact Assessments (PIAs)	The supplier can evidence that an appropriate PIA has been completed at the start of and was reviewed during the lifecycle of all change activity involving the Group's personal data. PIAs should include, as a minimum: • 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. GREEN = 100% RED = 99% or below -	Quarterly
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. GREEN = 100% RED = 99% or below 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.	Quarterly

	GREEN = 100% RED = 99% or below The supplier can evidence that equivalent contractual controls are in place with sub-processors. GREEN =100% RED = 99% or below	
Reporting of Data Privacy Breaches	The supplier can evidence that they report data privacy breaches to the Supplier Manager or direct to the GDPO as soon as they are identified and no longer than 24 hours after identification or in line with agreed contractual obligations. Review of breach log evidences reporting of data privacy breaches no later than 24 hours after identification. GREEN = 100% RED = 99% or below	Quarterly
Individual Rights Escalation	The supplier can evidence that they have escalated any individual rights requests (e.g. DSARs, portability, rectification) they cannot complete as part of business as usual processes to the Supplier Manager, relevant Group Business Owner or direct to the Group's Data Privacy & Records Management Team without delay and no more than 24 hours after receipt or in line with agreed contractual obligations. GREEN = 100% RED = 99% or below	Quarterly
Data Privacy Colleague Training	All supplier employees who have access to Group personal data must complete mandatory Data Privacy training within 8 weeks of commencing employment with the supplier and annually thereafter. GREEN = 90% RED = 89% or less	Quarterly
Record Type Schedule A Record Schedule of the Group's Records is in place and reviewed annually as a minimum.	The supplier can show evidence of how they have created and agreed with the Group a schedule of the Group's Records that it creates, store, processes, retains and disposes. The supplier can show evidence that it has quality reviewed the schedule annually as minimum.	Annually

(Applicable to supplier categories A, B, C, D)		
Creation and Retrieval Group Records are accurate and complete, reliable and usable and can be located and retrieved within 10 working days. (Applicable to supplier categories A, B)	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 (unless a Policy exception or Waiver is in place) and disposed of in a timely manner in line with the requirements of this Policy. (Applicable to supplier categories A, B, C)	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 (or evidence of Group sign off of an approved exception/waiver). 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 using a disposal log.	Semi-Annually
Legal Holds The supplier must be able to preserve Group Records upon request. (Applicable to supplier categories A, B, C)	The supplier can show evidence of how it applies legal holds/preservation notices issued by the Group. E.g. a procedure document and example of how this has been actioned (if applicable)	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 Lloyds Banking Group's Supplier Manager. The Supplier Manager will then discuss the non-compliance with the Accountable Executive for the relationship and local Risk team to agree way forward.

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