Group Personal Data Protection Compliance Policy

1. PURPOSE AND SCOPE OF POLICY

The purpose of this policy is to define the guidelines relating to the provisions of EU General Data Protection Regulation (hereinafter "Law"), which is applicable to the 27 EU member countries as of 25/05/2018, as well as the procedures and organizational responsibilities for their implementation, so as to ensure:

1. Consistency and transparency in the provision of all the principles under the Law;
2. Effective control over the implementation of the policy;
3. Time efficiency on all related processes;
4. Fair and lawful implementation in the context of the envisaged privacy culture;
5. Adherence to the protection of Personal Data of Customers, Prospect Customers, Suppliers, Business Partners and Employees (hereinafter "individuals"), and implementation of the relevant regulatory framework.

The scope of this policy is to enable Bank's employees to work effectively wherever and whenever in order to improve their working environment and be more productive and efficient. Any other issues relating to the specifics in regard to the DPIAs, specific procedures, and the data tool are not covered by this policy, so they are outlined in the relevant circulars.

2. ABBREVIATIONS

Within this document, the following abbreviations are used:

Abbreviation	Definition
BOC	Bank of Cyprus Group
CBC	Central Bank of Cyprus
CCTV	Closed Circuit Television
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
EU	European Union
GCD	Group Compliance Division
GDPR	General Data Protection Regulation
HR	Human Resources
IA	Internal Audit
IT	Information Technology
RCSA	Risk Control Self - Assessment
RoPA	Registry of Processing Activities
SCC	Standard Contractual Clause
ToR	Terms of Reference

3. DEFINITION OF TERMS

For the purposes of this policy, the terms listed below have the following meaning:

1. **Bank of Cyprus Group/BoC Group** means the Bank of Cyprus Public Company Ltd and its subsidiaries.

2. **Law** means the EU General Data Protection Regulation (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) as well as with the national legislation on the protection of personal data which is "The Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data" Law 125(1)/2018.

3. **GDPR** means the General Data Protection Regulation *(Regulation (EU) 2016/679)* as amended and replaced from time to time.

4. **Data Protection Impact Assessment** means an assessment by the Controller or Processor of the impact of the envisaged processing on the protection of Personal Data.

5. **Business partner:** Any third party, other than a client or supplier which has or had a business relationship or strategic alliance with the Bank (e.g. joint venture, joint development partner).

6. **Client:** Any third party that purchases, may purchase or has purchased a product or service from the Bank.

7. **Commissioner for Personal Data Protection:** The Commissioner for Personal Data Protection is appointed by the Council of Ministers and is responsible for monitoring the application of the Law and other provisions relating to the protection of individuals with regard to the processing of their personal data in Cyprus.

8. **Consent:** Any freely provided, express and specific indication of wishes in which one consents by a clear affirmative action, signifies agreement to the processing of his personal data.

9. **Controller:** The natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal data.

10. **Data Protection Officer [DPO]:** The data protection officer shall be designated on the basis of professional qualities and expert knowledge of data protection law and practices. The DPO must be involved in all issues relative to the protection of personal data, will be the liaison between the organization and the Commissioner of Personal Data Protection and will mainly inform and provide advice to those involved with personal data processing, amongst others.

11. **Data Subject:** The identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physiological, genetic, mental, economic, cultural or social identity of that natural person.

12. **Dependent:** The spouse, partner or child belonging to the household of the individual.

13. **Employee:** An employee, job applicant or former employee of the Bank. This term does not include people working at the Bank legal entities as external consultants or employees of Third Parties providing services to the Bank.

14. **Group:** Group shall mean Bank of Cyprus and all subsidiary companies or legal entities, including branches and representative officers.

15. **Individual:** Any Client, Supplier, Business Partner that is a natural person or any employee or any person working for a Client, Prospect Client, Supplier or Business Partner, including individuals whose personal data the Bank processes on the basis of a legal or contractual requirement towards a third party (e.g., beneficiaries, mandated persons or legal representatives).

16. **Personal Data:** Any information relating to an identified or identifiable natural person, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

17. **Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Failing to handle a data breach appropriately and in a timely manner may result in physical, material or non-material damage to data subjects, such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, amongst others.

18. **Processor**: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

19. **Processing:** Any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, view, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

20. **Pseudonymisation:** The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

21. **Sensitive Personal Data:** Personal data revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

22. **Staff:** All Employees and other persons who process personal data as part of their respective duties or responsibilities using the Bank information technology systems or working primarily at the Bank's premises.

23. **Supplier:** Any Third Party that provides goods or services to the Group (e.g., an agent, consultant, intermediary or vendor).

24. **Third party:** Any natural or legal person, public authority, agency, or body other than the Data

Subject, Controller, Processor or persons who are authorised to process personal data.

4. GENERAL PRINCIPLES

This policy elaborates the commitment of the **Bank of Cyprus Public Company Limited (hereinafter the 'Bank')** to adhere to the protection of Personal Data of Customers, Prospect Customers, Suppliers, Business Partners and Employees (hereinafter "individuals"), and implementation of the relevant regulatory framework. Protecting the security and privacy of personal data is important to the Group so as to conduct our business fairly and lawfully and in the context of the envisaged privacy culture. The policy is mainly based on the EU General Data Protection Regulation (hereinafter "Law") which is applicable to the 27 EU member countries as of 25/05/2018. The Law aims at harmonizing the rights and freedoms of individuals regarding processing of their personal data and ensures the free and protected flow of such data between Member States and equivalent countries. This policy has been fully implemented as of 25/05/2018.

Additionally, this policy complies with the Law as well as relevant guidelines issued by the Commissioner of Personal Data protection from time to time.

Bank of Cyprus Group operates in a constantly changing and demanding regulatory and supervisory environment.

Bank of Cyprus and its subsidiaries must, as a minimum meet the requirements of this policy. The policy is applicable for all subsidiaries of the Group as they are separate data Controllers. Therefore, roles and responsibilities defined in Appendix 1 should be adjusted accordingly at subsidiary level. The management of each entity is ultimately responsible for the implementation of this policy and to ensure, at entity level, that there are adequate and effective procedures in place for its implementation and ongoing monitoring to its adherence.

A. Principles for processing personal data

Each and every employee of the Bank should apply the following principles when processing personal data and the Bank should set out the relevant framework for adherence to these principles:

Legality (Lawfulness, Fairness, Transparency)	Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions mentioned in section B below is met and in the case of Sensitive Personal Data, at least one of the additional conditions set out below in section C is met**.**
Purpose	Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
Data Minimization	Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
Accuracy	Personal data shall be accurate and, where necessary, kept up to date.
Storage Limitation (Retention)	Personal data processed for any purpose or purposes shall not be kept for longer than what is necessary for that purpose or those purposes.

Accountability	Data Controller and data Processor are responsible and need to demonstrate and comply with the rights and principles of the Law.
Integrity& Confidentiality	Appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Transferability	Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

B. Lawfulness for Processing Personal Data

The Bank shall only collect, use or otherwise process personal data relating to Employees, Clients, Suppliers, Business Partners and sometimes non- clients (i.e. in order to handle complaints) if the processing falls within the scope of one (or more) of the purposes listed below.

I. For the performance of a contract

The Bank as data Controller processes personal data in order to perform banking transactions and offer financial services based on contracts with our clients and also to be able to complete our acceptance procedure so as to enter into a contract with prospective customers. The purpose of processing personal data depends on the requirements of each product or service and on the contractual terms and conditions which provide further details of the relevant purposes.

II. For compliance with a legal obligation

There are a number of legal obligations emanating from the applicable laws, with which the Bank is obliged to conform to, as well as statutory requirements, e.g. the Cyprus Banking law, the Money Laundering Law, the Cyprus Securities Law, Tax laws etc. There are also various supervisory authorities (e.g. the European Central Bank, the European Banking Supervisory Authority, the Cyprus Central Bank, Cyprus Securities Exchange Commission, European Investment Fund). Such obligations and requirements impose on the Bank personal data processing activities for credit checks, identity verification, tax law reporting obligations and anti-money laundering controls.

III. For the purposes of safeguarding legitimate interests

The processing of personal data is lawful so as to safeguard the legitimate interests pursued by the Bank or by a Third Party. A legitimate interest exists when the Bank has a business or commercial reason to use individual's information. However, even under such circumstances, the Bank must not unfairly go against what is right and best for the Data Subject. The Bank cannot assume it will always be appropriate for all processing operations. In order to base personal data processing on legitimate interests, extra responsibility is necessary for ensuring people's rights and interests are fully considered and protected.

This responsibility can be broken down into a three-part test:

- **Purpose test:** are you pursuing a legitimate interest?
- **Necessity test:** is the processing necessary for that purpose?
- **Balancing test:** do the individual's interests override the legitimate interest

The issue is further analyzed under the lawfulness of processing and through the DPIA process, where a legitimate interest test should be performed (using the relevant test tool) by the relevant stakeholder who has the ultimate responsibility for its sign-off. All legitimate interests performed should be recorded and publicized in the relevant privacy statements, in order to inform the Data Subjects and give them the opportunity to object to such processing.

IV. Individuals have provided their Consent

As long as an individual has provided his/her specific consent for processing then the lawfulness of such processing is based on that consent. Individuals have the right to revoke the said consent at any time. Before considering Consent as a legal basis to process personal data, it needs to be ensured that this Consent is specific, it is appropriately secured and adequately documented. Guidelines should be given on Consent management across the Bank to ensure proper understanding and management.

V. Necessary for the purpose of a public task

Processing is necessary for the performance of a task carried out in the public interest or that of an official authority whereby the Controller must adhere to.

VI. For the vital interests of the individual

When the processing is necessary in order to protect the vital interests of the data subject or of another natural person, for example if it's necessary to protect someone's life. This could be the life of the Data Subject or someone else.

When processing personal data, the Bank should decide which lawful basis for processing applies (Article 6) and should have relevant tools and guidelines to facilitate this. If none of the above purposes applies, then processing is not allowed.

C. Purposes for processing Sensitive Personal Data

The Bank is not allowed to process Sensitive personal data, unless one of the justifications enumerated in Article 9 of the Law is applicable. According to the Law, processing of Sensitive Personal Data is possible in the following situations:

- The Data Subject has given explicit Consent to the processing of such personal data for one or more specified purposes
- The data Controller, who is an employer, may process Sensitive Personal Data in so far as such processing is authorised by Union or Member State law or a collective agreement.
- Vital interests of the Data Subject or of another natural person are at stake.

D. Individual rights

The Bank maintains adequate procedures to ensure that:

i. all individuals are adequately informed of their rights and how to exercise them;
ii. properly written implementation procedures for each of the following Data Subjects' rights as described in Articles 12 to 22 of the Law regulation are in place

iii. the relevant procedures are executed at key touch points in the Bank, e.g. of all business lines, in order to be appropriately communicated to Data Subjects:

- The right to transparent communication.
- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure also known as 'the right to be forgotten.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- The rights in relation to automated decision making and profiling.
- The right to lodge a complaint**.**

Each Data Subject request is assessed and deliberated upon, based on its own merits by the Bank. All the procedures relating to Data Subject rights are analysed in the relevant circular (155).

E. Information to be provided and communication with Individuals

BOC is fully transparent and should develop and implement an effective data privacy communication plan to inform individuals as to the processing of their Personal Data.

Information to be provided must be:

- Communicated in a concise, transparent, intelligible way and be in an easily accessible form.
- Using clear and plain language, for any information addressed to a child (Article 12).
- In writing, or by other preferable means, including, where appropriate, by electronic means.
- Free of charge.

This information is usually provided via a Privacy Statement through all major points of contact with individuals (electronic or not) i.e. website, branch, 1Bank, Bank key customer documentation, job applications, contracts with external Processors etc. Privacy statements should be maintained and customized where necessary to adequately cover all service channels e.g. website privacy statement, customer privacy statement, Employee privacy statement etc. Additionally, the Bank should provide information about cookies, i.e. through a cookies policy, which contains information on how it uses them on the website and what options are available to individuals. All data privacy communication plans shall be updated at least on an annual basis or earlier, where deemed necessary, e.g. in case new service channels are introduced etc.

As a minimum a privacy statement should contain the following information:

- Identity and contact details of the Controller (and where applicable, the Controller's representative) and the Data Protection Officer.
- Purpose of the processing and the lawful basis for the processing.
- The legitimate interests of the Controller or Third Party, where applicable.
- Categories of Personal Data.
- Any recipient or categories of recipients of the Personal Data.
- Details of transfers to third country and safeguards.
- Retention period criteria.
- The existence of each of Data Subject's rights.
- The right to withdraw Consent at any time, where relevant.
- The right to lodge a complaint with a supervisory authority.
- The source the Personal Data originates from and whether it came from publicly accessible sources

- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

Procedures should be in place for individuals to communicate with the Bank and raise questions about the Bank's privacy procedures and principles. Contact details of the DPO should also be published (e.g dpo@bankofcyprus.com).

F. Data Breach Reporting

The Bank notifies the Commissioner within 72 hours of becoming aware of a data breach. Additionally, the Data Subject(s) affected should be informed when the breach is likely to result in a high risk to their rights and freedoms without undue delay. Relevant reporting criteria should be established towards this purpose. There should be an incident response plan in place for all breaches (operational, fraud, IT). All incident response plans should have provisions for notifying the DPO in case of a breach.

Vendors, who operate as Processors of Personal Data on behalf of the Bank, must notify the Bank without undue delay after becoming aware of a Personal Data breach, as per their contractual obligations.

G. Data Retention

The Bank retains data in accordance with the Law unless otherwise stated by other applicable laws, which may override the Law. The retention period should be aligned with the guidelines given by the local Commissioner for Personal Data Protection. Further details regarding the specific retention periods in the group can be found in the Information Security Policy and the Information Security Standard for Data Retention and the Historical Archive Data Preservation Policy.

H. External vendors

The Bank enters into agreements with Processors after providing sufficient guarantees that processing will meet the requirements of Law and ensure the protection of the rights of the Data Subjects and their Personal Data. Basic principles include:

- Processing shall be governed by a data processing agreement ('hereinafter the 'DPA'). The DPA should adequately and clearly delegate responsibilities and liabilities from the Controller to the Processor, and the vendor to acknowledge their responsibilities from controller to controller through the acknowledgement letter. In order to govern such processing, the relevant DPA between a Controller and the Processor, and an acknowledgement letter between a Controller and a Controller, must be signed. Relevant standard contract provisions shall exist, as per the European Commission's requirements when entering into an agreement with vendors outside the EU.
- Risk assessment of each vendor shall be performed and extended due diligence should be carried out based on this risk assessment in co-operation with the business owner of the contract. This applies to both existing and new external Processors. A contract may be terminated if the Processor cannot provide sufficient guarantees to safeguard Law requirements.
- Standard contractual clauses (hereinafter the 'SCC') for transfer for processors outside EU shall apply where applicable and the relevant link where the SCC are located is also included in the DPA.

The relevant privacy safeguards should be in place at the client onboarding stage as well as throughout the contract lifecycle in the Bank, and the relevant privacy forms and contracts shall be kept under a central depository.

The Bank should maintain a conclusive Law vendors management framework and develop tools for its implementation.

I. Data Protection Impact Assessment (DPIA)

The Bank shall maintain procedures to carry out DPIAs. DPIA supports the Bank in identifying potential data privacy risks and constitutes the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. The DPIA shall be initiated whenever a new process/ product or system that involves Personal Data is implemented and it shall be revisited/updated when there is a change in the risk profile of the process (e.g. new vendor, change of the procedure etc.). A DPIA should be carried out, in case there is processing of Personal Data, when:

- using new technologies and e.g., new systems, significant changes and digitization
- the processing is likely to result in a high risk regarding the rights and freedoms of individuals.

The DPIA should be repeated where applicable and based on the Bank's procedures.

All procedures relating to DPIA are analyzed in the relevant circular (O.E.180).

J. Transfer of Personal Data to Third Countries

Law imposes restrictions on the transfer of Personal Data outside the European Union, to third countries or international organizations. These restrictions are in place to ensure that the level of protection of individuals afforded by the Law is not undermined.

All cross-border transfers of Personal Data being to another Group legal entity, or a Third Party outside the EU (additionally including Iceland, Liechtenstein and Norway) must be covered by appropriate legal mechanisms. Data Processors must either reside in a country deemed adequate for data protection or offer guarantees satisfying EU laws and regulations on data protection, such as the SCC.

A third country may be declared as offering an adequate level of protection through an EC decision, when Personal Data can be transferred with another company in that third country without the data exporter being required to provide further safeguards or being subject to additional conditions.

In the absence of the above, a transfer can take place through the provision of appropriate safeguards and on the condition that enforceable rights and effective legal remedies are available for individuals. Such appropriate safeguards include:

- In the case of a group of undertakings, or groups of companies engaged in a joint economic activity, companies can transfer Personal Data based on the binding corporate rules which need to be approved by the competent data protection authority;
- Contractual arrangements with the recipient of the personal data, using, for example the SCC approved by theEC. The EC has adopted three sets of model clauses which can be found on the Commission's website (**https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en) ;**
- Adherence to an approved code of conduct or certification mechanism together with obtaining binding and enforceable commitments from the Controller or Processor in the third country.

- In the absence of an adequacy decision or of appropriate safeguards, the Personal Data may be transferred to a Third Party only under one of the following conditions:

i. The Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks;

ii. The transfer is necessary for important reasons of public interest, for the establishment, exercise or defense of legal claims, or in order to protect the vital interests of the Data Subject or of other persons.

K. Personal data transfers between the Group

Each company of the Group is a different legal entity acting as a separate Controller and there maybe cases that they share Personal Data for legitimate and lawful purposes. Such sharing will only take place, if necessary, safeguards exist for their protection which should be specified in writing. Additionally, Group companies should have in place service level agreements (hereinafter the 'SLAs') governing the transfer of data and their responsibilities.

L. Data Inventory

Every Controller is required to maintain a record of processing activities under its responsibility. This data inventory should be regularly updated and made available to the Commissioner for Personal Data Protection upon request. The Bank should set up a data mapping framework that will enable each company to match Personal Data to processes and facilitate the implementation of Law principles, such as the completion of DPIAs, which is to be facilitated through the relevant tool, in order to ensure it is maintained up to date.

Circular O.E.198 describes the recording of processes in the registry of processing activities tool

M. Other Principles

i. Marketing

The Bank shall only proceed to send to individual's unsolicited commercial communication (direct marketing communication) by obtaining the prior Consent of the individual ("opt-in"). In every direct marketing communication that is made to the individual, the individual shall be offered the opportunity to opt- out of further direct marketing communication. If an individual objects to receiving direct marketing communication from the Bank, or withdraws his Consent to receive such material, the Bank will take steps to refrain from sending further marketing material as specifically requested by the individual.

ii. Sanctions for non-compliance

Any breach of this policy will be regarded as a serious offence by the Bank, and it will result in disciplinary action. The Bank has procedures in place which enable it to take disciplinary action against employees who violate this policy.

If a person suspects any violations of this policy and wants to report it anonymously, this can be done through the whistleblowing line which is available to all members of Staff as per the Whistleblowing Policy and O.E. 128.

Non-compliance issues will be assessed accordingly, and relevant measures/processes should be in place to take into account the regulatory and reputational impact as well as the impact on the capital adequacy and liquidity of the Bank.

iii. Training

The Bank provides training on this policy and related data protection obligations to Employees, management & board members. In-depth trainings shall be provided on an ongoing basis to specific functions, more detailed trainings focusing on specific local requirements relevant for the compliance with this policy shall be provided on a local level. Furthermore, privacy culture has been enhanced to ensure that data is properly protected, and risks are minimized throughout the Bank.

iv. Employee Data Processing

Processing Personal Data in the employment context is performed according to the principles of the applicable law and with the aim of respecting the privacy of the employee. Processing operations must comply with the transparency requirements and employees should be clearly and fully informed of the processing of their Personal Data. Further details regarding employee data processing and employee rights and obligations can be found in the Employee Privacy notice and the Code of Conduct on portal.

v. Accountability

The Bank shall maintain adequate procedures to satisfy the Law accountability obligation. As Controllers the Bank implements appropriate technical and organisational measures (including introducing data protection by design and by default principles where relevant) to ensure and be able to demonstrate that data processing is performed in accordance with the Law.

vi. Security Measures

The Bank shall take appropriate commercial reasonable technical, physical and organizational measures to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, sorted or otherwise processed. To achieve this, the Bank shall develop and implement a relevant information security policy, standards, procedures and measures.

Employees shall be authorized to access Personal Data only to the extent necessary to serve the applicable legitimate purposes for which the personal data are processed by the Bank and to perform their job.

vii. Strategic Initiatives

The principles of this policy should be adequately adhered to during the implementation of new products and services, new outsourcing arrangements and projects of strategic initiatives i.e. sale of loans, restructuring of loans etc.

5. GOVERNANCE

5.1. Supervision and compliance

5.1.1. Board of Directors

The Board of Directors and Senior Management are responsible to oversee the Banks`s compliance with this policy. Additionally, they have the ultimate responsibility for implementation and adherence to this policy throughout the Bank, and the imposition of any remedial action.

Law touches upon every single area of the Bank and thus each and every member of Staff has a personal responsibility and obligation to implement this policy. Job responsibilities and enhanced roles are required so that Law requirements are adequately embedded into policies and procedures and become business as usual. Please refer to Section 5.2 for an overview of the respective responsibilities based on this policy.

5.1.2 Data Protection Officer (DPO)

BOC fully implements the requirement of Law to designate a DPO.

The DPO is responsible for supervising general compliance with Law and for advice on the implementation and interpretation of the policy throughout the Bank. DPO ToR, position and reporting lines are shown in Appendix 2 (DPO framework). The DPO is appointed officially by the Bank and his/her credentials are made known to the Commissioner of Personal Data Protection.

Collaboration of all designated DPOs for each Group subsidiary should exist to ensure conformity; consistency and efficiency (take advantage of all possible synergies where applicable). Furthermore, if there is a significant privacy incident**,** namely an incident affecting various systems used by the group or incidents that are generated by employees working in various companies, or risk that puts at stake the reputation of the Group etc. this should be escalated immediately to the DPO of BOC or even the Senior Management. The DPO of the Bank under her duties as Manager Data Privacy will exercise an oversight on the subsidiaries to ensure that the relevant policies and procedures are properly and timely applied by all subsidiaries (these duties are included in the role and responsibilities table section 5.2). Please refer to Appendix 2 for a more analytical overview of the respective DPO responsibilities based on this policy.

5.2. Roles and responsibilities

For the purpose of this policy, the following major Roles & Responsibilities have been identified:

Board of Directors & Senior management	The Board of Directors sets, approves and oversees the effective implementation of appropriate policies, practices and procedures to ensure compliance with the regulatory framework.
Audit Committee	The Audit Committee has the responsibility to approve this policy.
Data Protection Officer (DPO)	See Appendix 1 of this policy.
Manager Data Privacy	• Shares the annual action plan after it is approved by the Audit Committee with the subsidiaries to prepare their own action plan along the same lines. • Collects the privacy related information on a quarterly basis from the subsidiaries' DPOs to be included in the compliance quarterly report submitted to both the Audit Committee and Executive Committee • Ensures that the subsidiaries have equivalent procedures in place with those of the Bank to meet the privacy requirements • Exercise an oversight that this policy is applied by all subsidiaries via reviews.
Sourcing Procurement and Vendor Management	• Makes available and collects Law related contractual documentation to external vendors of the Group. • Maintains the list with all external Processors/vendors including the required Law classifications. • Maintains a list of SLAs of the Bank with Group companies and vice versa.

Line Directors	• Line directors have the ultimate responsibility and accountability for adherence to this policy within their divisions (as first Line of defence).
Regulatory Compliance Department	• Update this policy as and when required and monitor its high-level implementation.
Internal Audit (IA)	• IA includes this policy as an auditable area in its risk & audit universe and assesses the need for audit engagements during the annual audit planning process. The audit engagements planned by IA aim to assess the adequacy and effectiveness of relevant controls, in order to provide assurance in relation to the effective implementation of Law across the group.
Information Security	• Ensures that all security related Law principles are adequately reflected in the Information Security policy, standards and procedures. • Ensure that security incidents involving Personal Data breaches are timely and effectively reported to the DPO. • Supports Vendors Management risk assessment for information security
Information Technology	• Sets up and implement business requirements so as all systems support and implement the required Law principles and procedures. • Guides and facilitates the DPIA framework within the Bank. • Implements data minimization and data retention rules. • Implements controls to ensure the protection of Personal Data.
Legal	• Legal is responsible for providing general advice to the Bank on relevant legislation and for providing support, guidance and advice to departmental units/DPO in relation to legal issues and legal documentation including verification of correct legal basis, review of the Bank's Privacy Statement, contractual agreements etc.
Human Resource Division	• Internal HR procedures to ensure implementation of all Employee data privacy regulatory requirements and departmental procedures to ensure implementation of all Employee data privacy regulatory requirements. • Prepares and maintains the Employee privacy notice and facilitates and monitors its implementation. • Ensures that all privacy requirements are adequately reflected in the Employee privacy notice and the Code of Conduct. • Supports Employee privacy culture. • Supports and facilitates training on Law and data privacy in general.

Operational Risk Management	• Incorporates Law related compliance risk requirements into the RCSA assessment process. • Ensure that the new Products/Services Management Policy includes data protection related controls and evaluations and data privacy by design. Via the relevant circular it is required that the DPO must provide comments. • Incorporates DPIA procedural framework in the policy for new products and services. • Ensures that the feedback from the DPO based on DPIAs performed is taken into account during the RCSA process. • Ensures that incident reporting mechanism framework timely escalates data protection breaches incidents, and these are reported accordingly to DPO. • Raise issues related to GDPR and according to the methodology risk owners, • Maintain the data privacy risks in cooperation with DPO and Operational Risk Management.
Organization Department	• Identifies related cross functional procedures and updates them accordingly in co-operation with relevant owners so as to ensure that all the key principles of this policy are fully incorporated in all cross functional processes. • Incorporates all Law requirements in customer documentation as provided by Legal Dept and with the support of relevant departments. • Ensures that all the Law related policies are adequately reflected in written cross functional processes and procedures of the Bank. • Ensures adequate business-related requirements (not technical) are delivered to relevant departments e.g. IT to implement written cross functional processes. • Ensure adequate documentation for Consent management processes and relevant supporting procedures are updated to cover this in co-operation with relevant departments. • Support Corporate Affairs/DPO for internal communication of privacy related procedures and circulars. • Ensure relevant procedures are in place to support to DPIA process. • Ensure the implementation of circular O.E. 198.
Records Management	• Implements Law principles on non-automated records (e.g. hard copies)
Corporate Affairs	• Facilitates the external communication on Law issues that may include privacy notices, Law knowledge and actions to enhance the Groups privacy culture.
Historical Archive	• Ensures that Personal Data are maintained only after an appropriate Consent is obtained otherwise, they will be anonymized • Historical data as per Data Preservation Policy are minimized.

Process Owners (as per the definition in Circular 198)	• Record any new process (internal or cross-functional) under their responsibility. • Provide changes / updates to procedures in the RoPA tool. • Update their procedures at least every two years. • Perform the necessary DPIAs when needed (in cases when a DPIA is performed by another person / department, the evidence will be sent to the administrator who will register them as attached to the system and will update the procedure for conducting the DPIA.
All Staff	• Staff of the Bank is responsible for complying with this policy and its related procedures.

5.3. Supporting Documentation

This policy shall be reviewed annually and in consideration with the legislative or other developments, as appropriate. This policy is implemented via written procedures. For example, all the procedures relating to data protection are analysed in the relevant circular (O.E.155). The policy should be read in conjunction with the Information Security policy regarding protection issues. Presentations and informative material can be found on the Bank's portal under Compliance & DPO department. The Group shall develop and implement policies, minimum standards and procedures for adherence to this policy. This policy is related to a number of other policies or statements in the Group. As a rule, this policy provides the basis for other more detailed policies/documentation and organisational circulars, as seen in Section 6 (non-exhaustive).

6. IMPLEMENTATION PROCEDURES (KEY PROCESSES)

6.1 Supporting Procedures

- Privacy statement
- Lawfulness of processing and Consent guidelines
- Personal Data and Bank of Cyprus Group Circular (O.E.155)
- Circular on Data Privacy Impact Assessment (O.E 180)
- Procurement Circular (Κανονισμοί που διέπουν Προϋπολογισμούς & Δαπάνες) (O.E 89)
- Circular on Registry of Processing Activities -RoPA (O.E 198)
- Circular on Whistleblowing (O.E.128)

6.2 Supporting Policies

- Outsourcing Policy
- Employee Privacy Policy
- Code of Conduct
- Information Security Policy
- Historical Archive Data Preservation Policy
- Sourcing Procurement and Vendor Management Policy

Appendix 1

DPO framework in Bank of Cyprus under the GDPR

A. Designation of the DPO

BOC implemented fully the requirement of Law by designating a DPO. More specifically, the Controller (i.e. each entity such as BOC) and the Processor shall designate a DPO in any case where:

i. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity or
ii. the core activities of the Controller or the Processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of Data Subjects on a large scale; or
iii. the core activities of the Controller or the Processor consist of processing on a large scale of special categories of data pursuant to Article 9 and Personal Data relating to criminal convictions and offences referred to in Article 10.

Based on Law, a group of undertakings may appoint a single DPO provided that the DPO is easily accessible from each establishment. Group DPO for all Group entities is not recommended in the case of BOC Group due to (a) the size, differences and complexity of Personal Data held (b) different systems and procedures and (c) the requirement for the DPO to be easily accessible from each establishment (d) specialised knowledge is required on the business operations.

Based on the above criteria (criterion ii above) the Bank should designate a DPO. Furthermore, the following entities of the Group (as separate Controllers) should designate as a minimum a DPO:

i. Eurolife;
ii. GIC;
iii. CISCO;
iv. BOCAM
v. DEP

Bank of Cyprus Cultural Centre has appointed a separate DPO being a separate entity/foundation.

Collaboration of all designated DPOs should exist to ensure conformity; consistency and efficiency (take advantage of all possible synergies where applicable. Furthermore, if there is a significant privacy incident or a risk that puts at stake the reputation of the Group etc. this should be escalated immediately to the DPO of BOC or even the Senior Management.

Law (Articles 37-39) as well as the Guidelines on Data Protection Officer (WP 243) set out the tasks of the DPO as well as the Guidelines as to the skills, qualifications, and expertise of the DPOs required resources and envisaged position of the DPO. Please see in Table 1 (section the ToR and the responsibilities of the DPO as derived from the relevant framework).

B. Position of the DPO

I. Involvement of the DPO in all issues relating to the protection of Personal Data

Article 38 of the Law provides that the Controller and the Processor shall ensure that the DPO is 'involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data'.

II. Independence and reporting lines of DPO

Article 38(3) states the following safeguards should exist to enable the DPO to act in an independent manner:

- Does not receive any instructions regarding the exercise of [his or her] tasks.
- He or she shall not be dismissed or penalised by the Controller or Processor for performing his/her tasks. This requirement strengthens the autonomy of DPOs and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks.
- No conflict of interest with possible other tasks and duties (as per below).
- The DPO shall directly report to the highest management level of the Controller.

Assignment and Reporting lines

Upon the assignment of the DPO at each Controller/Processor level it is important to ensure and guarantee that his/her reporting lines enable him/her to perform their tasks with a sufficient degree of autonomy and fulfil his/her duties in an independent manner. More specifically, prior to the assignment of a DPO both the reporting lines and the DPO authority/mandate should be reviewed together as both elements are equally important and hold one another in balance to ensure sufficient operational independence and authority.

Reporting lines are also subject to the reporting structure of the Controller and Processor as long as the above requirements are satisfied in relation to independence The DPO may report to a senior member of the management team e.g., director for administrative matters (budgets, staffing, absences, sick leave approvals). The reports via the Compliance Director to the Audit Committee of the Board to take additional strategic decisions e.g. approval of overall GDPR program and DPO action plan, acting as a catalyst in case conflicts/disagreements arise from the first line of reporting.

Such direct reporting ensures that Senior Management and the Board of Directors is aware of the DPO's advice and recommendations as part of the DPOs mission to inform and advise the Controller or the Processor. Therefore, direct access of the DPO to Senior Management and the Board of Directors is important.

As a minimum the report (at least on an annual basis) of the DPOs activities should be submitted to the highest management level (i.e. Board of Directors or Committee of the Board).

The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39. The Controller or Processor remains responsible for compliance with Law and must be able to demonstrate compliance. If the Controller or Processor makes decisions that are incompatible with the Law and the DPO's advice, the DPO should be given the opportunity to take his or her dissenting opinion clear to those taking the decisions.

DPO should be appointed officially by the Bank and his/her credentials are made known to the Commissioner of Personal Data Protection.

III. Conflict of Interest

Briefly, the Law states that the DPO must not be conflicted by having a dual role of governing data protection whilst also defining how data is managed. DPOs are allowed to have other functions provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organization that leads him or her to determine the purposes and the means of the processing of Personal Data. Due to the specific organizational structure in every company of the Group, each case must be considered separately.

Conflicting positions within the organization may include senior management positions (such as Chief Executive, Chief Operating Officer, Finance Director, Director of Corporate Affairs, Chief of Staff, or Chief Information Officer) but also other roles if such positions or roles lead to the determination of purposes and means of processing. In addition, conflicts of interests may also arise for example if an external DPO is asked to represent the Controller or Processor before the Courts in cases involving data protection issues.

IV. Accessibility and localisation of the DPO

According to Section 4 of the Law, the accessibility of the DPO should be effective**.**

C. Required skills for the DPO

The DPO *'shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39*'. The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the Personal Data being processed. For example, where a data processing activity is particularly complex, or where a large amount of Sensitive Personal Data is involved, the DPO may need a higher level of expertise and support.

The necessary skills and expertise include:

- expertise in national and European data protection laws and practices including an in-depth understanding of the Law,
- understanding of the processing operations carried out,
- understanding of information technologies and data security,
- knowledge of the business sector and the organization,
- ability to promote data protection culture within the organization.

D. Resources of the DPO

Article 38(2) of the Law requires the organization to support its DPO by 'providing resources necessary to carry out their tasks and access to Personal Data and processing operations, and to maintain his or her expert knowledge'. The following items are to be considered:

- Active support of the DPO's function by senior management (e.g. at board level).
- Sufficient time for DPOs to fulfil their duties.
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
- Official communication of the designation of the DPO to all Staff to ensure that their existence and function are known within the organization.
- Necessary access to other services, such as HR, legal, IT, security, etc., so that DPOs can receive essential support, input and information from those other services.
- Continuous training. DPOs must be given the opportunity to stay up to date regarding developments within the field of data protection.
- Given the size and structure of the organization, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up.
- In general, the more complex and/or sensitive the processing operations are, the more resources must be given to the DPO. The data protection function must be effective and sufficiently well-resourced in relation to the data processing being carried out.
- DPO function to be supported by detailed procedures to support the implementation of this framework.

TERMS OF REFERENCE-

DATA PROTECTION OFFICER (DPO)

In summary the tasks (as a minimum) of the DPO include:

i.	to inform and advise the Controller (BOC) or the Processor and the employees who carry out processing of their obligations pursuant to G D P R and to other Union or Member State data protection provisions.
ii.	to monitor compliance with GDPR , with other union or member state data protection provisions and with the policies of the Controller or Processor in relation to the protection of Personal Data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; As part of its duties to monitor compliance with Law, DPOs may, in particular: • collect information to identify processing activities • analyse and check the compliance of processing activities • inform, advise and issue recommendations to the Controller or the Processor
iii.	to provide advice where requested as regards the DPIA and monitor its performance pursuant to Article 35; More specifically the Controller should seek the advice of the DPO, on the following issues, amongst others: • whether or not to carry out a DPIA • what methodology to follow when carrying out a DPIA • whether to carry out the DPIA in-house or whether to outsource it • what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the Data Subjects • whether or not the DPIA has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the Law.
iv.	to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 and to consult, where appropriate, regarding any other matter.
v.	Article 37(7) of the Law requires the Controller or the Processor to publish the contact details of the DPO and to communicate the contact details to the relevant supervisory authorities. The objective of these requirements is to ensure that Data Subjects (both inside and outside of the organization) and the supervisory authorities can easily, directly and confidentially contact the DPO without having to contact another part of the organization. This means that a procedure should be set up by the DPO to fulfil these responsibilities.
vi.	DPO shall in the performance of his or her tasks, have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing'.

In essence, it requires DPOs to prioritize their activities and focus their efforts on issues that present higher data protection risks. This does not mean that they should neglect monitoring compliance of data processing operations that have comparatively lower level of risks, but it does indicate that they should focus, primarily, on the higher-risk areas.
vii. DPO to be seen as a discussion partner within the organization and that he or she is part of the relevant working groups dealing with data processing activities within the organization. Consequently, the organization should ensure, for example, that: • The DPO is invited to participate regularly in meetings of senior and middle management. • His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner to allow him or her to provide adequate advice. • The opinion of the DPO must always be given due weight. • The DPO must be promptly consulted once a data breach or another incident has occurred.
viii. Co-operates with DPOs of other Group companies to disseminate knowledge and expertise, maximize synergies and deal with intra-group Law compliance issues.
ix. The DPO is ultimately responsible for ensuring maintenance of data inventory records in compliance with applicable requirements. The DPOs need to be able to demonstrate that each firm comprising the Group compliance with Article 30 of the Law, i.e. that each firm maintains an accurate and up to date inventory that captures the Personal Data processing within the firm. (The Controller or the Processor, not the DPO is required to 'maintain a record of processing operations under its responsibility' or 'maintain a record of all categories of processing activities carried out on behalf of a Controller')
x. Ensures that there is a well-established procedure for data breaches and that all data breaches are timely reported.
xi. Ensures that the data privacy complaints are investigated in an adequate and timely process and are part of the current complaints handling procedure.