State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Privacy by Design Assessment Report

National Data Privacy Office

This report is autogenerated based on the responses filled by the respective assessors using the beta version of the Privacy by Design Assessment Tool developed by the National Data Privacy Office (NDPO).

Please note that the results presented in the report are not verified by NDPO and should be merely viewed as guidance and does not certify compliance with Privacy by Design principles.

Disclaimer:

This Privacy by Design Assessment report has been generated using a tool intended to provide a snapshot of the current state of privacy by design practices implemented in the in-scope application, and therefore the report should not be considered as legal advice or a definitive assessment of compliance.

The information presented in this report is based on the data and settings provided at the time of generation and may not capture changes or developments that occur after this report's creation. Furthermore, the accuracy and completeness of the report may be influenced by the accuracy and completeness of the input data.

The creators and providers of this tool, Qatar National Data Privacy Office (NDPO), disclaim any liability for the use or interpretation of this report and do not assume any responsibility for the consequences of decisions or actions taken based on the information contained herein. Organizations are ultimately responsible for their privacy practices and compliance efforts by regularly reviewing and updating relevant privacy policies and practices to maintain ongoing compliance.

By using this report, you acknowledge and accept these terms and limitations.

Gap descriptions and recommendations are provided exlusively for controls that are either ineffective or parially effective. When dealing with partially effective controls, it is important to note that there may be uncertainity regarding their exact level of effectiveness. As a result of which, the same gap descriptions and recommendations are applied to both ineffective and partially effective controls.

Recommendations in the report are based on good practices and will require to be tailored/customized based on the system/application's technology and privacy landscape. It is the responsibility of the organization to implement the controls and any liability arising out of incorrect implementation is not the responsibility of NDPO.

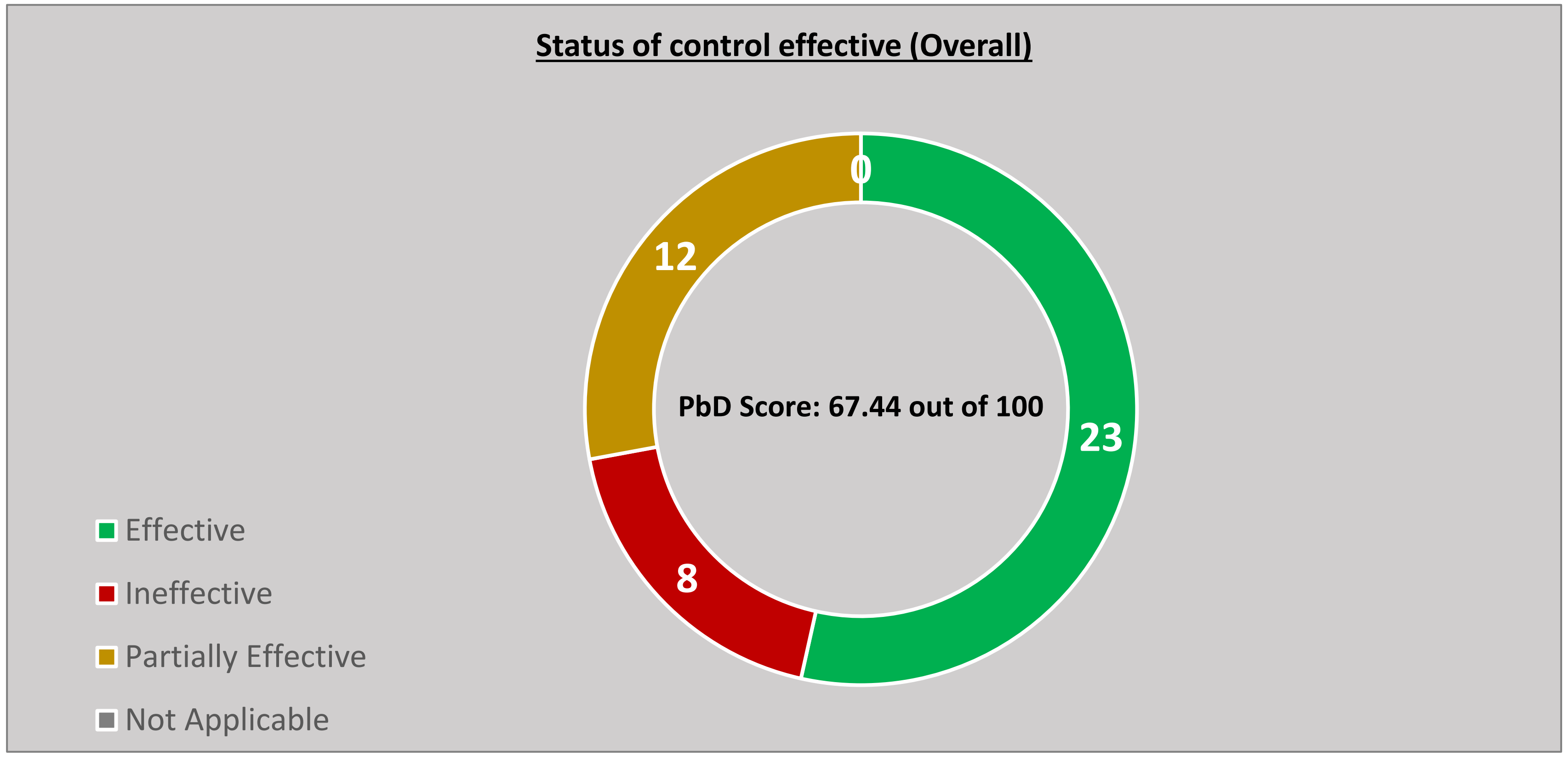
Contents of the Report:

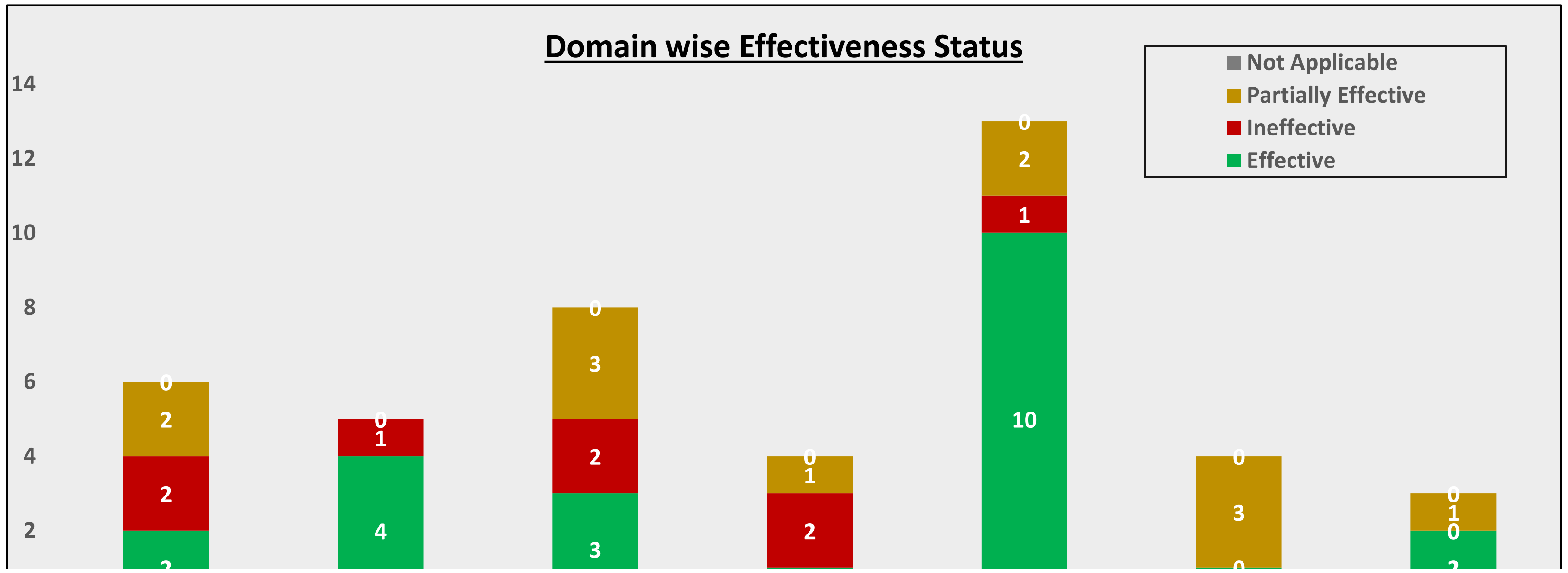
The report contains the following sections:

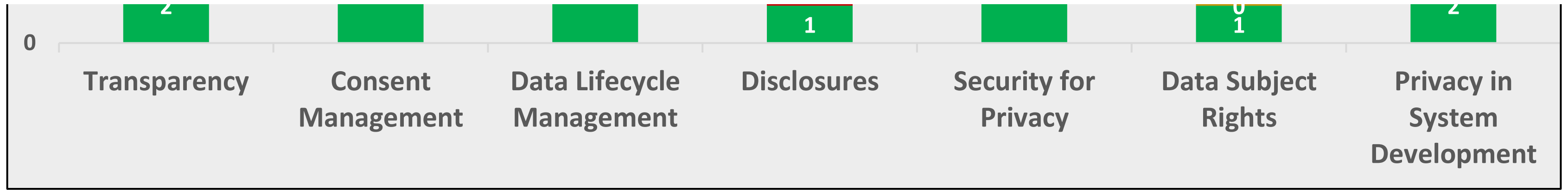
Overview about the Application

NAME OF THE APPLICATION	PayPal
NAME OF THE ORGANIZATION	PayPal Holdings, Inc.
DETAILS OF THE ASSESSOR	Hafsa Farhan, Eiman Iftikhar
DATE OF THE ASSESSMENT	26 June, 2024
DETAILS OF PROCESSING ACTIVITIES CARRIED OUT	Account registration, transaction processing, user verification, device and usage data, customer support
PERSONAL DATA ATTRIBUTES PROCESSED	Full names, Account Information, Financial Information, Identification number, data and usage information.
LIST OF UPSTREAM AND DOWNSTREAM APPLICATIONS	Downstream Applications are Mobile Apps, Merchant Websites, POS systems and Upstream Applications are Banking systems, Credit card networks and identity verification services.
APPLICATION HOSTING DETAILS	Hosted on PayPal's own data centers and cloud service providers across various locations to ensure redundancy and compliance with regional data protection laws.
APPLICATION ARCHITECTURE	Microservices architecture
THIRD PARTIES INVOLVED	Paypal companies including Venmo,Paypal Honey,Legal Authorities,Paypal Credit,Paypal Savings, Paypal Cashback Mastercard ,PayPal Extra Mastercard, Card networks and payment processors, Fraud prevention,identity verification, Credit reporting and debt collection agencies.Service Providers and other Paypal Users and Merchants.

Assessment Results - Dashboard


Status of control effective (Overall)


Domain wise Effectiveness Status



PRIVACY BY DESIGN ASSESSMENT - FINDINGS AND PROPOSED WAY FORWARD

Gap ID	Gap	Gap Description	Recommendation
G_01	Privacy Notice	The system/application does not have the functionality in place to present the users (individuals) with a Privacy Notice at the time of collecting their personal data.	It is recommended to the perform the following: - Develop a Privacy Notice template to describe the processing of personal data by the system/application and in accordance with PDPPL and other applicable regulatory requirements. - Subject the Privacy Notice template to appropriate review mechanisms. - Publish the Privacy Notice on the system/application. - Identify all points of data collection within the system/application. - Present the users (individuals) with a Privacy Notice across all points of data collection. For further reference: Privacy Notice - Guideline for Regulated Entities
G_02	Updated Privacy Notice	There is no process in place to notify the individuals on changes in personal data processing activities via an updated Privacy Notice.	It is recommended to the perform the following: - Update the existing Privacy Notice template to reflect the changes in personal data processing activities. - Subject the Privacy Notice template to appropriate review mechanisms and incorporate review comments. - Publish the updated Privacy Notice on the system/application. For further reference: Privacy Notice - Guideline for Regulated Entities

G_03	Updated Privacy Notice - Prompt	There is no process/functionality in place to either redirect the individuals to the updated Privacy Notice upon their first access post updating the Privacy Notice or send email communications to individuals on the updates made to the Privacy Notice.	It is recommended to perform the following: Option 1: Implement a functionality in such a manner that the system/application prompts the users (individuals) to review and accept the updated Privacy Notice through a privacy banner. (AND/OR) Option 2: Send email communications to all registered users (individuals) on updates made to Privacy Notice contents either manually or via an email gateway. For further reference: Privacy Notice - Guideline for Regulated Entities
G_04	Cookie Policy	There is no functionality in place to present the individuals with a Cookie Policy.	It is recommended to the perform the following: - Develop a Cookie Policy template to describe how the system/application uses cookies. - Subject the Cookie Policy template to appropriate review mechanisms and incorporate review comment. - Publish the Cookie policy on the system/application. Guidance on Cookie policy contents: It is recommended to cover the following as part of the cookie policy: - What types of cookies do you use? - What personal data do the cookies process? - What are the purposes of these cookies? - How long will they track the individuals? - How can individuals opt-in or opt-out of cookie usage?
G_05	Cookie Consent Banner	There is no functionality to present individuals with a cookie consent banner upon their first access.	It is recommended to perform the following: - Implement a functionality to present the users (individuals) with a cookie consent banner and prompt the individual to select their cookie preferences on their first access. - Ensure that the web application stores only necessary cookies on the individuals device (and not other types of cookies), prior to obtaining consent.

G_06	Collection Limitation	There are no checks in place to limit the collection of personal data to what is adequate, relevant and necessary.	It is recommended to perform the following: - Identify all processing activities that are carried out using the system/application. - Review if the processing activities are in accordance with the privacy notice and cease those processing activities which are not listed in the Privacy Notice. - Identify all personal data attributes that are captured by the system/application. - Review if the personal data fields that are captured by the system/application are necessary for the processing activities and remove any excessive data fields. For further reference: Principles of Data Privacy - Guideline for Regulated Entities
G_07	Purpose Limitation	There are no checks in place to limit the collection of personal data.	It is recommended to perform the following: - Identify all processing activities that are carried out using the system/application. - Review if the processing activities are in accordance with the privacy notice and cease those processing activities which are not listed in the Privacy Notice. For further reference: Principles of Data Privacy - Guideline for Regulated Entities
G_08	Data Minimization	There is no process in place that limits the usage of personal data to what is adequate, relevant and necessary.	It is recommended to perform the following: - During the design stage of the system/application, identify all proposed processing activities that may be carried out using the same. - Identify only those personal data attributes that are necessary for carrying out the proposed processing activities. - Obtain a buy-in from the privacy team for using the identified personal data attributes for the proposed activities. - Ensure that the system processes only requisite personal data attributes for carrying out the approved processing activities. For further reference: Principles of Data Privacy - Guideline for Regulated Entities

G_09	Retention Period	Retention periods are not defined for personal data processed using the system/application.	It is recommended to perform the following: - Identify all personal data processed by the application/system. - Identify and finalize the retention period for each of the personal data attribute processed by the application/system depending on business requirement and/or legal requirement. Factors such as data sensitivity, industry specific regulations and contractual obligations should be factored in. - Retention periods identified should be defined and documented in a retention schedule. For further reference: Principles of Data Privacy - Guideline for Regulated Entities
G_10	Retention Policy Enforcement	Retention policy is not enforced on the system/application.	It is recommended to perform the following: - Develop a well-defined retention policy framework that outlines the retention periods, procedures, and responsibilities for enforcing data retention within the system/application. This policy should be documented, communicated to relevant stakeholders, and periodically reviewed and updated to reflect changing regulations or business needs. - Implement technical controls within the system/application to enforce the defined retention periods. This may involve configuring automated mechanisms, such as data archiving, backup systems, or data lifecycle management tools, that can facilitate the timely deletion of data based on the established retention policies. - Privacy Office along with Internal Audit Team should periodically monitor compliance of the application/system to the retention policy. For further reference: Principles of Data Privacy - Guideline for Regulated Entities

G_11	Data Processing Agreements	There are no Data Processing Agreements executed with Third Party processors have access to personal data processed by system/application.	It is recommended to perform the following: - Identify all Third Parties that may have access to personal data processed by the system/application. - Review the existing contractual agreements with the identified Third Parties (in Step 1), to evaluate if they contain relevant Privacy and Data Protection Clauses in accordance with PDPPL agreements and identify the contracts which do not contain adequate provisions. - Update the contractual agreements which do not contain adequate provisions from a Privacy and Data Protection standpoint by ensuring clauses around the following are included: a) Purpose and scope of processing b) Data Processing Instructions c) Data Protection and Security measures d) Sub processing. For further reference: Controller and Processor - Guideline for Regulated Entities
G_12	Notify individuals of disclosures	There is no process to notifies users on the disclosure of their personal data to third parties.	It is recommended to perform the following: - Identify all Third Parties that may have access to personal data processed by the system/application. - Update that the Privacy Notice (linked to the system/application) with the list of Third Parties which may have access to personal data processed by system/application.
G_13	Limit usage of Third Parties	There is no process to ensure personal data is disclosed to third parties only for carrying out personal data processing activities stated in the Privacy Notice.	It is recommended to perform the following: - Identify all personal data processing activities (using the system/application) carried out by the Third Parties. - Verify if the identified processing activities falls within the processing activities stated in the Privacy Notice.
G_14	Data Backups	Critical data residing on the system/application is not backed up.	It is recommended to perform the following: - Identify and finalize the following factors with regards to data back ups: i) critical data that is required to be backed up. ii) frequency of backups iii) reliable and secure backup storage location iv) backup method to be used v) appropriate backup tools or software. - Backup the data based on the above finalized factors.

G_15	Incorrect Logon Attempts	Users/non users are able to attempt to log on to an account for an unlimited number of times, making it more possible for non-users to guess password	It is recommended to perform the following: - Define a threshold value for the number of incorrect logon attempts depending on the criticality of system/application. - Define the account lockout policy in such a manner that it locks out the user's account temporarily for a specific duration or indefinitely until intervention by an administrator. - Implement the account lockout policy on the system/application accordingly.
G_16	Patching	Critical vulnerabilities are not patched without undue delay.	It is recommended to perform the following: - Implement a process for prioritizing vulnerabilities that require patching basis their severity. - Implement a centralized patch management system that performs timely patching of critical vulnerabilities across all systems and applications. - Perform a periodic review to ensure all critical vulnerabilities are patched accordingly.
G_17	DSR - Access	System/Application and the underlying databases do not have the functionality to search and retrieve a copy of personal data.	It is recommended to perform the following: - Develop a data search mechanism that allows for the requested individual's data to be located within the system/application and it's underlying databases. - Upon locating the requested data, retrieve and convert the same to machine-readable format. For further reference: Individuals' Rights - Guidelines for Regulated Entities
G_18	DSR - Correct	System/Application and the underlying databases do not have the functionality to search, update and amend personal data.	It is recommended to perform the following: - Develop a data search mechanism that allows for all the instances of requested individual's data to be located within the system/application and it's underlying databases. - Upon locating the requested data, amend all instances of the data as per the request received. For further reference: Individuals' Rights - Guidelines for Regulated Entities

G_19	DSR - Delete	System/Application and the underlying databases do not have the functionality to search and delete personal data.	It is recommended to perform the following: - Develop a data search mechanism that allows for all the instances of requested individual's data to be located within the system/application and it's underlying databases. - Upon locating the requested data, delete all instances of the data as per the request received. For further reference: Individuals' Rights - Guidelines for Regulated Entities
G_20	Testing	There is no process to ensure production data are not used for testing purposes.	It is recommended to perform the following: - Finalize the data set that is going to be subject to testing purpose and identify all personal identifiers contained in the same. - Prior using the dataset for testing, ensure that all personal data identifiers are removed or replaced with synthetic data.

Thank You!

This report has been created using the "Privacy by Design" assessment tool, a product of the Qatar National Data Privacy Office (NDPO) aimed at advancing the adoption of the "privacy by design" approach within Qatari organizations. Your valuable comments and feedback are encouraged and can be directed to privacy@ncsa.gov.qa. We appreciate your engagement.