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

Contents of the Report:

The report contains the following sections:

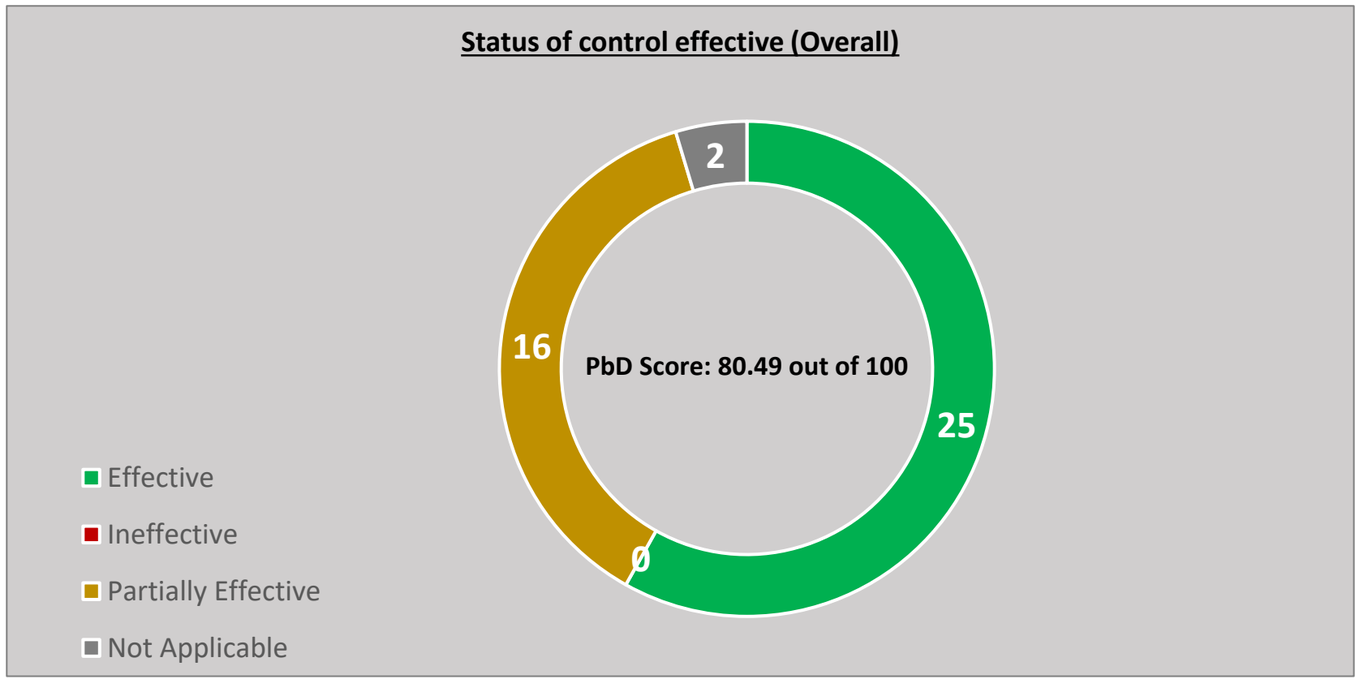
1. Overview about the Application and Assessment - Page 3

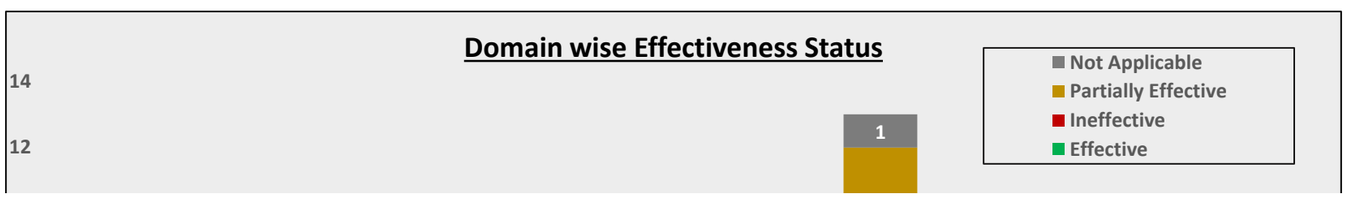
2. Assessment Report - Dashboard - Page 4

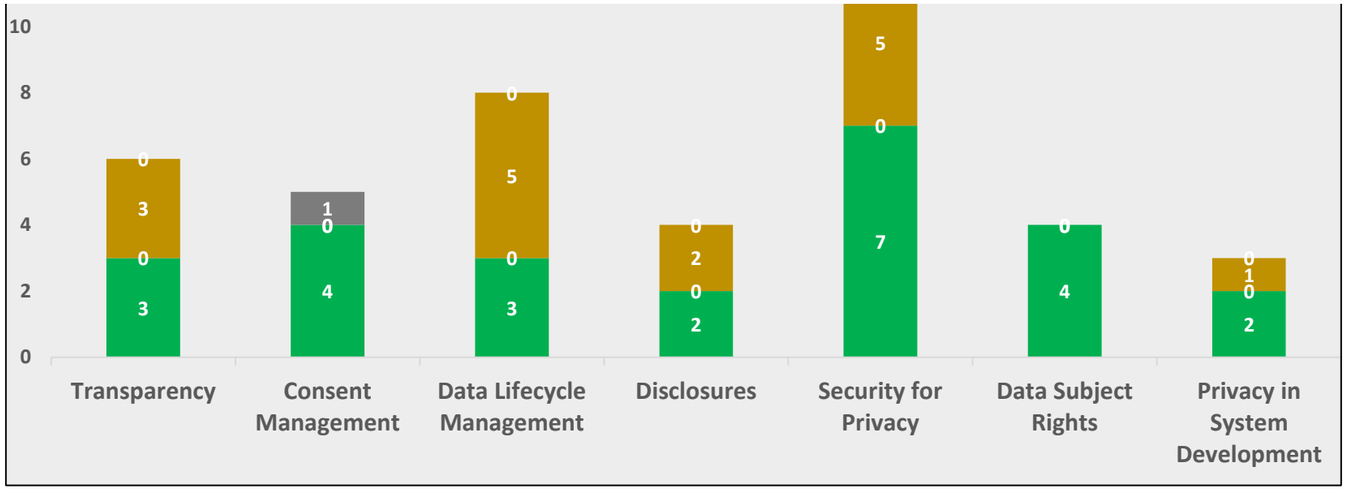
3. Privacy by Design Assessment - Findings and way forward - Page 5

Overview about the Application	
NAME OF THE APPLICATION	Uber
NAME OF THE ORGANIZATION	Uber Technologies, Inc.
DETAILS OF THE ASSESSOR	Ali Ranjbar (student), Almabrouk Ben-Omran (student), Mohammed Ashjar (student).
DATE OF THE ASSESSMENT	16/05/2024
DETAILS OF PROCESSING ACTIVITIES CARRIED OUT	Account Creation and Management, Location Tracking and Sharing, Ride History and Preferences, Payment Processing, Communication and Notifications, Identity Verification, Feedback and Ratings, Customer Support, Marketing and Promotions, Analytics and Performance Monitoring, Compliance and Legal Requirements, Accessibility and Special Needs
PERSONAL DATA ATTRIBUTES PROCESSED	Name, Phone number , Email, Location, Payment information (optional), Profile photo, Travel history, Device information, Audio recording (optional), Emergency Contacts (optional).
LIST OF UPSTREAM AND DOWNSTREAM APPLICATIONS	1- Upstream apps: Google Maps API, Apple Pay, Google Cloud Platform, Firebase Cloud Messaging, Mapbox, Stripe, PayPal, Google Pay, Onfido, Jumio, Amazon Web Services, OAuth, Firebase Authentication, Twilio. 2- Downstream apps: Uber Rider App, Uber Driver App, Uber's Internal Analytics Tools, Google Analytics, Mixpanel, Amplitude, Zendesk, Salesforce Service Cloud, Braze, HubSpot, Uber Eats, Uber Freight, Jump Bikes, Government and Regulatory Reporting Tools, Audit Tools, Concur, TripActions.
APPLICATION HOSTING DETAILS	Uber's application is hosted across multiple cloud providers like Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI)
APPLICATION ARCHITECTURE	Uber started with a monolithic architecture but has transitioned to a Domain-Oriented Microservice Architecture (DOMA)
THIRD PARTIES INVOLVED	Payment Processors, Mapping and Navigation Services, Third-party Service Providers, Government and Regulatory Authorities, Marketing and Advertising Partners, Business Partners and Affiliates, Acquirers or Mergers

Assessment Results - Dashboard







PRIVACY BY DESIGN ASSESSMENT - FINDINGS AND PROPOSED WAY FORWARD

Gap ID	Gap	Gap Description	Recommendation
G_01	Privacy Notice - Contents	There is no process in place to ensure Privacy Notice adheres with the requirements of PDPPL.	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. - Update the Privacy Notice template based on review comments. - Publish the Privacy Notice on the system/application. 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	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_04	Records/Inventory	Personal data inventories are not developed for processing activities carried out using the system/application.	It is recommended to perform the following: - Identify all processing activities carried out using the system/application. - Develop a Record of all the identified processing activities by inventorizing all personal data attributes processed by the system. - Review and update the Records of processing activity on a periodic basis. For further reference: Record of Processing Activities - Guideline for Regulated Entities
G_05	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_06	Data Accuracy	There are no measures in place to ensure accuracy of personal data is maintained.	It is recommended to perform the following: - Provide a functionality for the individuals to review and update their personal information. - Send a periodic reminder to the individuals to review and update their personal data. For further reference: Principles of Data Privacy - Guideline for Regulated Entities
G_07	Anonymization	Anonymization/de-identification is not performed.	It is recommended to perform the following: - Privacy Office along with relevant stakeholders (eg. owners and users of Applications and Systems, BU Heads) should determine if there are any use cases for Anonymization/De-identification of personal data contained in the application/system. - Upon identification of use cases, relevant technique for data anonymization (such as Data Masking, Generalization, Data swapping, Data perturbation, etc.) should be identified - Perform data anonymization in accordance with technique identified. - Perform periodic reviews to inspect if the anonymization technique is implemented adequately.
G_08	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_09	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_10	Limit disclosure of personal data attributes	There is no process to limit the disclosure of personal data attributes to what is necessary.	It is recommended to perform the following: - Identify all personal data processing activities (using the system/application) carried out by the vendors and the purpose for carrying out the same. - Identify the personal data attributes disclosed to the vendor for fulfilling the purpose for which they are carrying out personal data processing activities. - Assess the necessity for disclosure of every single personal data attribute and identify redundant personal data disclosures. - Restrict the disclosure to only those attributes that are necessary by removing all redundant personal data disclosures.
G_11	Access controls	There is no process that restricts data access only to authorized personnel	It is recommended to perform the following: - Leverage RBAC principles to define roles and associated access privileges within the application and identify the different roles that require access to personal data. - Assign access permissions to each role based on their job responsibilities and the principle of least privilege. - Implement robust user authentication mechanisms to verify the identity and authorization of users accessing the application.
G_12	Audit Logging	Audit logging is not enabled on the system/application.	It is recommended to perform the following: - Identify and finalize the specific activities and events that need to be logged such as user logins, data access, modifications, configuration changes, failed login attempts, and administrative actions. - Design the logging system to capture relevant information (timestamp of the event, user ID, the IP address or device identifier, the action performed, etc.) about each logged event. - Securely store the logs (for a defined time period) to safeguard them from unauthorized access, tampering, or deletion. - Regularly review and analyze the audit logs to identify any suspicious activities and anomalies.
G_13	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_14	Idle Session Timeout	Sessions do not expire upon inactivity for a certain period of time.	It is recommended to perform the following: - Define a session timeout policy for the system/application depending on its criticality (idle time session time out must be low for critical systems/applications and high for lesser critical systems/applications). - Implement a mechanism to track user activity and update the session status via running server side tracking or client side scripts. - Implement a mechanism to log out the user from the system/application in accordance with the session timeout policy.
G_15	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_16	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.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

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.