**APPENDIX 1**

# Technical Specifications

# Business Rules

1.1 The scope of this Request for Proposal (RFP) is limited to the payment gateway processing prepaid recharges only.

No changes or modifications are to be made to the existing online recharge procedures at Alfa's side.

The proposed solution should seamlessly integrate with the current online recharge system and processes without any disruption.

Bidders are expected to focus solely on the replacement, enhancement, and optimization of the payment gateway, ensuring compatibility and coexistence with the existing procedures and infrastructure. *(K)*

Bidder to allow customization of the Payment Gateway page look and feel.

1.2 Bidder to advise on field requirements (mandatory/optional) and implement a clear visual indicator for mandatory fields on the payment page.

1.3 The payment gateway interface and user messages should be available in English.

1.3.1 The solution must support the ability to add additional languages such as French and Arabic with the ability to easily switch languages during the checkout process.

1.4 Bidder to share detailed list of Error and Successful messages scenarios.

1.4.1 MIC1 shall have to right to review and customize messages displayed to end users.

1.4.2 Bidder to provide context-specific error messages for different scenarios to minimize customer confusion and prevent potential complaints.

1.5 After a successful recharge, customer receipt shall be clearly provided to customers on a separate landing page. *(K)*

1.5.1 Bidder to provide the possibility to save and print the receipt.

1.5.2 Bidder to provide a sample of customer receipt.

1.6 The bidder should present a user-friendly approach for displaying errors to end-users if applicable and describe the logging mechanism for system administrators to efficiently identify and address errors. *(K)*

1.7 MIC1 reserves the right to decide whether errors should be displayed on the gateway or within the Alfa system.

1.8 The solution must support recurring recharges through tokenization for secure and convenient repeat payments.

1.8.1 Provide comprehensive information on tokenization options, including a detailed explanation of all supported functionalities and behaviors.

1.8.2 Allow customers to store and manage up to X cards, with the option to designate a preferred card for default use.

1.8.3 Possibility to define scheduled reccurrent recharges (B-number and recharge type).

1.8.3.1 schedule based on fixed dates.

1.8.3.2 schedule based on regular intervals (x days) with an end date.

1.8.3.3 schedule based on regular intervals (X days) without end date.

1.8.3.4 schedule and personalize recharges for up to [n] B-numbers, each with its own recurrence/frequency.

1.9 Bidder to list and support major card providers including but not limited to:

1.9.1 Visa

1.9.2 Mastercard

1.9.3 American Express (Amex)

1.9.4 Discover

1.10 Additionally, the bidder is required to provide support for integration with leading E-Wallet services.

1.11 The bidder is required to integrate both 3D secured cards and non-3D secured cards.

1.1 This integration should facilitate seamless transactions while ensuring the necessary security measures are in place for both card types.

1.2 The bidder must provide detailed documentation on how they plan to implement and manage these card types within the proposed solution.

1.12 The payment gateway interface should be fully responsive and optimized for seamless user experience across various devices and screen sizes:

1.12.1 desktop

1.12.2 mobile

1.12.3 tablet

1.12.4 Specify any limitations or specific platform requirements.

1.13 The payment gateway interface and functionality must be compatible with:

1.13.1 all major browsers including but not limited to:

1.13.1.a Chrome

1.13.1.b Edge

1.13.1.c Firefox

1.13.1.d Safari

1.13.2 all major operating systems:

1.13.2.a Windows

1.13.2.b macOS

1.13.2.c Linux

1.13.2.d iOS

1.13.2.e Android

1.13.3 Specify any limitations or specific platform requirements.

1.14 Bidder shall provide a comprehensive and proactive chargeback management strategy, outlining specific procedures for prevention, detection, and resolution ensuring timely and effective responses.

1.15 Bidder shall abide by Alfa's restrictions regarding allowed currencies. For example, current rules: *(K)*

- Lollar not allowed

- Fresh dollar cards

- LBP payment only for Lebanese cards issued from Lebanese banks: payment to be based on Sayrafa daily rate or any official exchange rate adopted as communicated on Alfa's website.

# IT Specs & Acceptance

2.1 Payment gateway should be secured using SSL certificate HTTPS to encrypt the data exchanged between Alfa channels and the payment gateway. This ensures the security of sensitive information such as credit card details.

2.2 Payment gateway should provide various types of integration that best fit Alfa business such as hosted checkout.

2.3 Payment gateway should provide API access for integration such as RESTful APIs that can be used to send and receive payment information securely.

2.4 Payment gateway's API should be compatible with any programming language such as .Net, java or php.

2.5 Payment gateway should provide list of APIs not limited to: *(K)*

1-Create Order Request

2- Retrieve Order Details

3- Cancel Order

4- Refund Order

2.6 Payment gateway should provide documentation for Development integration and testing guides.

2.7 Payment gateway should provide sample code for integrations based on any programming lanaguage such as .Net, java or php

2.8 Payment gateway should implement webhook support to send Alfa channels real-time updates from the payment gateway. Webhooks are essential for handling events such as successful payments, refunds, or chargebacks.

2.9 Implement robust error handling to manage situations such as declined transactions, connection issues, or other errors that may occur during the payment process.

2.10 Payment gateway should provide a sandbox or testing environment where we can simulate transactions without processing real payments. Using this environment to thoroughly test our integration before deploying it in a live environment. *(K)*

2.11 Payment Gateway should provide clear description of all possible response codes returned for any transaction.

2.12 Payment Gateway should allow us to specify for each transaction the return url that should be redirected to after completion of payment on hosted checkout. *(K)*

2.13 Payment Gateway should have the ability to specify whether many or single attempt is allowed on Hosted checkout before returning to the specified return url.

2.14 Payment Gateway should show meaningful error messages when many attempts are allowed for single transaction. These messages to be customized based on Alfa needs for each response code.

2.15 Payment Gateway should provide a gateway web interface for admin where admin can create users and specify the roles and privileges on gateway interface.

The web interface should perform all needed actions based on user's profile/privileges and not limited to: *(K)*

1- define users and roles

2- search for online recharges with different search criteria

3- make refund

4- extract reports

2.17 Payment Gateway should have the possibility to send email notifications for payments. The list of recipients should be managed by gateway interface.

2.18 Payment Gateway should have control over the session timeout of the hosted checkout. This expiry of session should be well known and less than certain number. This number should be set by alfa on gateway interface.

2.19 Payment Gateway should have control over the number of transactions performed by the same IP Address during a specific period of time. This number should be set and defined by alfa.

2.20 Vendor shall describe the testing strategy that will be used during the project to guarantee the final result.

2.21 Test Plan: Vendor shall deliver a Test Plan describing the strategy followed for testing: test objectives, test environment, test resources requirements, duration for tests, test tools needed.

2.22 Test Design: Vendor shall deliver a Test Design Document including all the needed test cases in order to assure that the system is fit for purpose and fit for use.

2.23 Acceptance Report: Vendor shall deliver an Acceptance Report detailing the execution phase, reporting remaining issues/defects.

2.24 MIC1 reserves the right to add or modify the test plan and acceptance report to include additional or missing objectives, requirements, and acceptance criteria.

2.25 MIC1 will include its requirements (functional testing, integration testing, regression testing, training…) and reserves the right to require additional tests to verify the correct installation/integration in the network.

2.26 Acceptance tests will be performed to determine if the system delivered meets the required and specified accuracy, throughput, functionality, and business requirements specified.

2.27 Implementer certified engineers shall be present during the performance of each system acceptance test. In no way shall the bidder deviate from the systems acceptance test plan negotiated.

2.28 MIC1 reserves the right to conduct additional tests at any time during the life of the project without any additional cost.

2.29 Implementer shall prepare and document containing validation and test plans for the acceptance phase, including expected results and validation/ testing techniques for accuracy, throughput, functionality and all other requirements, Fault and error cases, Performance and load tests, Testing of all the provided tools.

2.30 The bidder shall perform all system acceptance validation/ testing in accordance with the MIC1 approved test plans.

2.31 MIC1 will review the results of the validation and provide an acceptance or rejection letter signed by the proper MIC1 authority and addressed to the bidder.

2.32 It’s only after the bidder receives MIC1 acceptance letter that the requirements will be considered as completed and accepted.

2.33 These test plans shall indicate what requirements will be validated in conjunction with the bidder prior to usage verses those requirements validated through daily usage by MIC1 staff and personnel.

2.34 The bidder shall provide a full and complete audit trail for all system and solution acceptance validation / testing and the requisite reports from this audit trail.

2.35 All plans must be approved by MIC1 prior to acceptance testing and shall be contract deliverables.

2.36 Errors detection scenarios: Testing should intentionally attempt to make things go wrong to determine if things happen when they should not or things do not happen when they should. In this area test boundary conditions should be included in acceptance tests and should cover all data flows integrated.

2.37 Provisional acceptance (PA) granted once major defects are resolved and no known critical issues are affecting normal business operations.

2.38 Final Acceptance (FA) granted 3 months after PA, if :

all punch list items of the PA have been cleared and only in case during these 3 months no service affecting fault occurred and the Bidder fixed all support relevant issues within the Service Level Agreement to be defined."

# Fraud Control

3.1 The payment gateway must include a robust online and flexible Fraud Prevention System (FPS) to quickly detect fraudulent transactions and accommodate to fraudsters pattern changes without putting our line of business at risk. *(K)*

3.2 The solution must keep proactively monitoring, analyzing the data and enhancing the rules to reduce fraud rate and false positives, minimize chargeback and increase acceptance rates.

3.3 We shall transfer all online recharge transactions to be processed and monitored by the payment gateway fraud system as main functionality.

3.4 The fraud system must be functioning in real time monitoring mode.

3.5 The fraud system must be based on advanced technologies of fraud detection and prevention (i.e customer profiling,machine learning and artificial intelligence)

3.6 The fraud system must support combination of flexible rules and behavioral self-learning analysis to detect anomalies in transaction for maximum fraud prediction accuracy.

3.7 Bidder must specify the fraud chargeback ratio.

3.8 The bidder must be committed to ongoing improvement of the fraud prevention system.

3.9 The solution must be capable to analyze historical transaction data for identifying patterns and trends.

3.10 Bidder shall specify the duration for which historical data will be retained. This is crucial for detecting long-term patterns and trends.

3.11 The bidder must specify the methods used for risk scoring transactions.

3.12 The bidder must specify the methods of alert notification, including email, SMS, or other channels.

3.13 The solution must accept immediate rule changes to be applied when agreed between parties.

3.14 When fraudsters make it hard and plays around the rule limits, system must be able to cope with such hard changes and detect such fraud without affecting genuine cases. i.e fraudsters highly rotate IP address using automated software to send a low volume of requests per IP potentially evading rate limiting rule; the same apply to other element monitoring that fraudster tries to cope with its limit.

3.15 Solution must support monitoring the phone number as part of single/combined rule configuration and behavior analysis. Phone number will be sent as encrypted value.

3.16 The solution shall support:

3.16.1 Rule monitoring for LBP and $ separately

3.16.2 When needed,rule monitoring in one currency (i.e $) where one of the currency is converted into the other (LBP to $) based on official agreed exchange rate

3.16.3 Monitoring rules at request level and not post-authorization even when to check 3DS

3.16.4 When needed,monitoring rules post-authorization with instant automatic reversal amount in case transaction was blokced

3.16.5 Rule configuration to include the transaction status (decline/success)

3.16.6 Monitoring element with combined rules 2 or more (i.e monitor phone number when count transactions>x and count distinct cards >y)

3.16.7 Rules in passive mode for monitoring purposes for new and historical data

3.16.8 Specific rule and threshold configuration based on BIN type (local/international) and currency

3.16.9 Dynamic and calendar monitoring period type depending on the needs

3.16.10 Not blocking a transaction if one rule is violated but once more than 2 rules are violated (i.e count per day and count per month breached) when needed

3.16.11 Detecting any sequential pattern used within a certain period (IP,card..etc). Bidder shall explain how the system identifies and responds to such patterns within a specified period

3.16.12 Monitoring changes in geolocation or sudden shifts to new devices can be indicative of potential fraudulent

3.16.13 Defensive mecanism for Bot attack

3.16.14 Capability to detect simultaneous transactions within milliseconds

3.16.15 Online daily monitoring to our merchant transactions must be carried by the supplier's team where any deviations must be immediately analyzed while informing Alfa with the analysis outcome and recommendations.

3.17 Supplier must provide list of merchant rule functions, elements and monitoring period that can be configured not limited to the below required :

3.17.1 Rule function:

3.17.1.1 Total Amount

3.17.1.2 Count transaction

3.17.1.3 Distinct values

3.17.2 Elements:

3.17.2.1 Device fingerprint (web/mobile app)

3.17.2.2 IP

3.17.2.3 Card

3.17.2.4 Phone Number (encrypted value with long character)

3.17.2.5 Email

3.17.2.6 BIN

3.17.2.7 Card holder name

3.17.2.8 BIN Country

3.17.2.9 IP Country

3.17.3 Rule function:

3.17.3.1 Hour

3.17.3.2 Week

3.17.3.3 Bi-week

3.17.3.4 Month

3.18 Supplier to specify that the solution can accept future elements which can be mapped to certain data fields and then build on monitoring rules.

3.19 Bidder to specify what elements for fraud monitoring are required from Alfa other than email, phone number, channel (web/mobile) transaction amount and currency.

3.20 Solution to allow blacklist of the below not limit to:

3.20.1 BIN

3.20.2 BIN country

3.20.3 IP

3.20.4 IP country

3.20.5 Email:

3.20.6 Phone Number

3.20.7 Device FingerPrint

3.21 Solution must allow whitelist when needed.

3.22 The system must support at least the below rule functions and elements monitoring:

3.23 Criteria to be added to the rule are not limited to: period , currency ,transaction status , local /international BINs, IP country:

3.16.23.1 Device Fingerprint:

3.16.23.1.1 Count transaction per Device fingerprint

3.16.23.1.2 Total amount per Device fingerprint

3.16.23.1.3 Count distinct phone number per Device fingerprint

3.16.23.1.4 Count distinct emails per Device fingerprint

3.16.23.1.5 Count distinct IP countries per Device fingerprint

3.16.23.1.6 Count distinct cards per Device fingerprint

3.16.23.1.7 Count distinct Card BINs countries per Device fingerprint

3.16.23.2 Card:

3.16.23.2.1 Count transaction per card

3.16.23.2.2 Total amount per card

3.16.23.2.3 Count distinct cardholder names per card , using fuzzy word matching and non-case sensitive

3.16.23.2.4 Count distinct phone number per card

3.16.23.2.5 Count distinct emails per card

3.16.23.2.6 Count distinct IP countries per card

3.16.23.3 Email:

3.16.23.3.1 Count distinct cards per email

3.16.23.3.2 Count distinct Device Fingerprint per email

3.16.23.3.3 Count distinct phone number per email

3.16.23.3.4 Count distinct IP Countries per email

3.16.23.3.5 Count distinct Card BINs countries per per email

3.16.23.3.6 Count transactions per email

3.16.23.3.7 Total Amount per email

3.16.23.4 Phone Number:

3.16.23.4.1 Count distinct cards per phone number

3.16.23.4.2 Count distinct Device Fingerprint per phone number

3.16.23.4.3 Count distinct emails address per phone number

3.16.23.4.4 Count distinct IP Countries per phone number

3.16.23.4.5 Count distinct Card BINs countries per phone number

3.16.23.4.6 Count transactions per phone number

3.16.23.4.7 Total Amount per phone number

3.16.23.5 IP:

3.16.23.5.1 Count distinct cards per IP

3.16.23.5.2 Count transactions per IP

3.16.23.6 Cardholder name:

3.16.23.6.1 Count distinct cards per Cardholder name for international cards

3.24 System to allow configuration of combined rules not limited to the below examples:

3.24.1 Count transanctions>x and count distinct cards >y per phone number within a day for non Lebanese cards using $ currency.

3.24.2 Count of distinct phone number >x and cumulative amount >y per email address within a day for non Lebanese cards using $ currency and for successful transactions.

3.25 At least, for the above rules samples , their thresholds and elements are to be configured per merchant ID and not global.

3.26 Bidder to specify the rule functions that are configured globally but cannot be configured by merchant.

3.27 System must be flexible to set up customized rules based on fraud future changes.

3.28 System must provide analytical summary dashboard with dynamic charts and filters.

3.29 Alfa User must have a GUI access to generate at least all the below required analytics and reports.

3.30 Alfa User must have the option to filter by currency to view the below dashboard and reports.

3.31 Dashboard and reports must have many filter options with any of the available detailed/summary fields.

3.32 Alfa User must have the option to select the columns to populate in the report and save this selection for the future.

3.33 Detail and summary data retention to be available for 12 months.

3.34 Charts and data behind dashboard to be exportable into excel as charts and not only as picture.

3.35 All summary analytical dashboard and below required reports/stats to show data as of today (online) and by custom date.

3.36 Detailed transaction report to be exported for a month at least in one shot with no limitation.

3.37 All below dashboard and reports requirements to be populated by currency.

3.38 Analytical Dashboard to show:

3.38.1 Daily approval rate %, Total Daily transaction sales, Total Amount per day

3.38.2 The above to be updated once user chooses Week, Month or year.

3.38.3 Comparative bar chart showing total number of accepted vs declined vs blocked count of transaction per day if week filter is selected; then by month if month filter is selected.

3.38.4 Comparative bar chart showing total amount of accepted vs declined vs blocked amount per day if week filter is selected; then by month if month filter is selected.

3.38.5 Supplier must support his feedback with samples of what is required.

3.39 Detail Transaction Report:

3.39.1 Transaction details report showing at least :Transaction number,card number(6 digits masked), card holder name, card type(Visa/Mastercard..etc), date and time(Beirut time), amount, currency,transaction status(declined, accepted),issuer error message,BIN,BIN country, IP,IP country,device fingerprint,email,mobile phone number,bank name, fraud decision (blocked,passed,monitored),rule name violated (separated by a delimiter) ,browser used,3DS flag.

Bidder to confirm if all above fields are available in one report.

3.39.2 When querying transactions details, we should be able to filter by Date & Time,transaction number, transaction status(accepted,declined,blocked,monitored,refunded or all), Payment amount (specific or range ),Currency,Card type (Visa/Mastercard..etc),payment channel (Mobile,Web),acquirer name,devicefingerprint,card number,email,IP,IP country,BIN country before populating the result.

Bidder to confirm that at least all the above are applicable to filter

3.39.3 Report to be exportable to excel, pdf and csv.

3.39.4 Supplier must support his feedback with samples of what is required.

3.40 Rule performance report:

3.40.1 Summary of rule performance showing total transactions, transactions accepted, and their %, transaction rejected, and their %, transaction monitored and their %

3.40.2 Drill down to Rule performance details where report must show:

3.40.2.1 Rule Name, count transactions triggered, count transactions rejected by the rule, % rejected, count monitored, % monitored.

3.40.2.2 Report to be exportable to excel, pdf and csv.

3.40.3 Supplier must support his feedback with samples of what is required.

3.41 System must support showing below summary within certain period (Day,week,month) represented into graphical way :

3.41.1 Most BIN countries used with amount and count.

3.41.2 Most IP countries used with amount and count.

3.41.3 Most failure transactions reasons with amount and count.

3.41.4 Most email used with amount and count.

3.42 Supplier must provide list of other system available dashboard and reports with samples.

3.43 System must allow user to build his own detail/summary reports, based on the available detail data fields.

3.44 System must support saving the customized reports templates for scheduled runs.

3.45 System must support saving the chosen filter for fast future use.

# Customer Care

4.1 The selected payment gateway partner is expected to take ownership of and promptly address customer complaints, particularly those related to payment card issues, demonstrating a commitment to effective customer care and issue resolution.

4.2 The bidder is requested to include a dedicated interface for customer care within the proposed solution.

4.3 This interface should be designed to enhance customer support and communication, allowing efficient handling of inquiries, issue resolution, and overall customer satisfaction.

4.4 The bidder is required to provide detailed specifications and functionalities of the customer care interface, demonstrating its effectiveness in addressing customer needs and facilitating a positive user experience.

# Finance

5.1 Payment gateway should have the following fields (date of transaction / transaction reference /amount of transaction / currency / card number / status of transaction).

5.2 Search criteria based on transaction id.

5.3 Search criteria based on card number.

5.4 Functional ability to perform refund transactions. *(K)*

5.5 Historical transactions should be accessible once needed.

5.6 All data should be exported to excel.

5.7 Reports generated based on two criteria ex (date and status of transaction).

5.8 Bidder shall support reports cut off (daily at night) at the time defined by alfa.

5.9 Bidder shall commit to abide by alfa's payment and settlement methods regarding used currencies. For instance, amounts collected in USD should be settled to alfa in fresh USD, and amounts collected in LBP should be settled in LBP or in USD based on a rate defined and approved by Alfa.

5.10 To provide business training for the reporting and refunding process including but not limited to a complete training for the interface provided for such purposes.

# Information Analytics

6.1 The bidder is expected to strictly adhere to Alfa's comprehensive security standards throughout the entire duration of the project. These standards encompass, but are not limited to:

- data encryption protocols,

- access controls,

- network security measures,

- Predefined API

- etc.

6.2 For the claim procedure: full MSISDNs will never be provided; instead, hashed MSISDNs should be shared.

6.3 The generated transaction must include the Payment card number.

6.4 The communication between payment gateway and Alfa network must be through predefined API and passes through middleware.

6.5 Low level design and the integration with Alfa network must be shared, including transactions flows.

6.6 The bidder should provide a sample of the shared reports between the supplier and Alfa team.

# Reporting

7.1 The system shall feed the datawarehouse with a structured data format events.

7.2 Events description shall be provided in terms of fields type and values.

7.3 Solution shall be able to sftp events to datawarehouse server.

* 1. MIC1 shall be able to specify Filenaming convention and distribution frequency.

# Information Security Specifications

1 The Bidder shall commit to refrain from offering any product / equipment which can cause security threat or information leakage that jeopardizes MIC1 network security. *(K)*

2 The Bidder shall accept that MIC1 runs a vulnerability scan on the proposed solution prior to issuing the acceptance and in case any vulnerability is found, the Bidder undertakes to take the necessary actions to remedy such vulnerability within 15 days from its notification. *(K)*

3 The Bidder shall mention the security standards adopted/followed in designing the proposed solution.

4 The Bidder should specify if it has acquired the ISO27001 certification or any other equivalent security certification and submit with the Offer a copy of such certificate.

5 The Bidder shall not hard code passwords in the proposed solution. *(K)*

6 The provided application should run without the need of root (unix) and / or admin (win) privileges.

7 System shall allow generation of admin, user as well as alarms logs.

8 The Bidder should submit a data flow diagram and schema of the solution architecture.

9 The Bidder shall harden the solution before being published online, and describe hardening aspects, security checking and audits performed.

10 The Bidder shall change default system errors / messages and configuration and implement proper error handling to prevent the exposure of sensitive information in error messages.

11 Encryption shall be used in all communications / interactions between systems. Access shall always be used through HTTPS. End-to-End Encryption ensures that sensitive data is encrypted from the point of entry (e.g., customer's browser) to the point of processing. *(K)*

12 Least-privileges should always be specified on nodes / applications.

13 Pseudocode flow chart shall be provided by the Bidders.

14 The Bidder should commit to improve solution / systems information security weaknesses whenever needed or highlighted by MIC1 information security team. *(K)*

15 Supplier will suggest any additional security plan that should be applied from the server side.

- Server will communicate only with external Whitelisted IPs.

- Port whitelisting

- WAF with custom Rules

- DDoS attack prevention

- all communication to be done over https

- encryption of personal information APIs

16 Two-Factor Authentication (2FA): Enforce two-factor authentication for payment processing for all card types. This adds an extra layer of security.

17 Supplier should undergo regular security audits to ensure the robustness of their systems.

18 Supplier Regularly update the payment gateway integration, APIs, and any related software components to patch known vulnerabilities and enhance security.

19 Supplier should adhere to the OWASP Top 10 vulnerabilities as a baseline for secure development.

20 The payment gateway provider must demonstrate compliance with the Payment Card Industry Data Security Standard (PCI DSS) to ensure the secure processing, storage, and transmission of cardholder data.

21 The payment gateway service should offer the capability to tokenize sensitive payment data, replacing it with unique identifiers (tokens) to minimize the storage and transmission of sensitive data across systems.

22 The payment gateway provider must support two-factor authentication for secure access to the administrative interface, ensuring an additional layer of protection against unauthorized access.

23 The payment gateway service should incorporate robust fraud prevention and detection mechanisms, including real-time transaction monitoring, IP geolocation, velocity checks, and integration with trusted third-party fraud detection services.

24 The payment gateway provider must offer secure APIs for integration with our systems and applications, adhering to industry best practices for authentication, authorization, and data encryption.

25 The payment gateway provider should undergo regular security audits and conduct penetration testing to identify vulnerabilities, ensuring the effectiveness of their security controls.

26 The payment gateway provider must comply with relevant data protection regulations, including but not limited to the General Data Protection Regulation (GDPR) or other applicable regional data privacy laws, to ensure the protection and lawful processing of customer data.

27 The payment gateway provider must have a well-defined incident response process and a clear policy for timely and transparent breach notification in the event of any security incidents or data breaches.