Customer Privacy and Security Notice

Disclaimer

CUSTOMER PRIVACY NOTICE

This Privacy Notice is related to the collection, use, processing and sharing of your personal data, including sensitive personal data, by any member of Eazy Financial Services ("Eazy").

The Data Manager of your personal data is Eazy, you have or may have a relationship with. Eazy is committed to ensuring that your personal data is protected under Bahrain Personal Data Protection Law (PDPL) (Act No. 30 of 2018).

1. DETAILS ON HOW WE COLLECT YOUR PERSONAL DATA

1. Eazy collects your personal data directly from you via different communication channels such as emails, phone calls, face-to-face meetings or online during registration process and completion of application forms, in the payment process, and during your engagement with Eazy to provide you with services
2. Eazy also collects your personal data indirectly from Internet, social media, public records, and Third-party service providers.

2. THE LAWFUL BASIS FOR PROCESSING YOUR PERSONAL DATA

Eazy only processes your personal data including sensitive personal data based on lawful basis under Bahrain PDPL and your consent to Eazy to process personal data and share internally with Eazy's subsidiaries when there is a legitimate business interest and with third parties when required by the law, or where it is necessary to administer the relationship or where Eazy has another legitimate interest in doing so.

3. AUTOMATED DECISION MAKING AND PROFILING

Eazy may take decisions based on automated processing of personal data including profiling of an individual or group.

4. TYPES OF PERSONAL DATA WE PROCESS

Based on the specified lawful reasons of processing your personal data, Eazy may handle and process your:

1. Identity details: full name, contact details including telephone numbers and email addresses, gender, marital status, family details, job title(s), location of birth, photograph, video.
2. Address details: residential address, employer address, correspondence address.
3. Identification details: identification numbers issued by government bodies (for example: CPR, passport copy, driver's license number, other government-issued identity number).
4. Financial information: bank account information, income, and other financial information.
5. Anti-fraud data: details about fraud convictions, allegations of crimes and sanctions details received from various anti-fraud databases, or regulators or law enforcement agencies.
6. Sensitive personal data such as ethnicity, religion, and criminal records.

5. PERSONAL DATA SHARING

Eazy may share your personal data including sensitive personal data for the below mentioned reasons:

1. Internally with Eazy's subsidiaries when there is a legitimate business interest.

2. With third parties when required by the law, or where it is necessary to administer the relationship with you or where we have another legitimate interest in doing so. These third parties include external auditors, system support vendors, and governmental bodies and may include the following:
   a. Third Party Service Providers
   b. Banks to process payment transactions including online payments
   c. Attorneys for managing court cases between you and Eazy

6. SECURITY OF YOUR PERSONAL DATA

Your personal data will be processed as per Eazy's Personal Data Protection Framework. We use reasonable and appropriate measures to protect your personal data from unintentional or unauthorized destruction, accidental loss, unauthorized alteration, disclosure or access, or any other form of processing, taking into account the risks involved in the processing and the nature of the personal data.

7. RETENTION PERIOD OF YOUR PERSONAL DATA

Eazy retains your personal data based on legal retention period requirements, the validity of the contract, fulfilling its intended purposes, and historical archiving. We securely destroy and erase or anonymize your personal data to ensure that it cannot be restored after exceeding the specified retention period. In the majority of cases this will be for minimum of ten years from the end of your relationship with Eazy.

8. YOUR RIGHTS AS A DATA OWNER

You have the right to request Eazy to:

1. Access your personal data processed by Eazy
2. Change your personal data when it is inaccurate or incomplete
3. Remove, block, or restrict your personal data when:
   a. Purpose of personal data is no longer valid
   b. Processing of personal data is unlawful
   c. Processing of personal data lacks the legitimate interest of Eazy
   d. Deletion is necessary for compliance with the law
   e. Personal data is inaccurate
   f. You wish to withdraw your consent
4. Submit an objection when personal data is used for:
   a. Direct marketing
   b. Processing that may result in defamation or discrimination causing possible financial or emotional loss
   c. Decision making and the decision is taken based only on automated processing
5. Withdraw your consent at any time to process or transfer your personal data for a specific reason

Eazy has the right to reject your request. Eazy will inform you about the rejection along with the reason for rejection within 15 business days of receiving the request. In case your request is incomplete, Eazy will inform you within 10 days of receiving the request to complete your request. Further, you have the right to complain to Bahrain Personal Data Protection Authority/Ministry of Justice.

9. YOUR ROLE TO KEEP YOUR PERSONAL DATA ACCURATE

It is essential for Eazy to keep your personal data up to date and accurate. Therefore, kindly provide your updated information in case there is any change to your personal data during your business relationship with us.

10. UPDATE ON PRIVACY NOTICE

Eazy has the right to review and update the privacy notice. In case of any changes, we will inform you of any substantial change in how we process your personal data.

CUSTOMER SECURITY NOTICE

11. PHYSICAL SECURITY

1. Merchants have custodial responsibility for their mobile device used as Point-of-Sale terminal.
2. Merchant must not leave the mobile device used as Point-of-Sale terminal unattended without ensuring prudent security measures.
3. Merchant must not allow others to perform any activity on their mobile device used as Point-of-Sale terminal.
4. Merchants are responsible and liable for all actions including transactions performed on their mobile device used as Point-of-Sale terminal.
5. Merchant must verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
6. Merchant must be aware of suspicious behaviour around device (for example, attempts by unknown persons to open devices).
7. Merchant must not install, replace, or return devices without verification.
8. Merchant must promptly report loss of mobile device used as Point-of-Sale terminal to Police and Eazy Financial Services.

12. PASSWORD

1. Merchant is personally responsible for safeguarding his/her account and log-in information.
2. Merchant must not permit another person to log-on to their mobile device used as Point-of-Sale terminal utilizing their account and log-in information.
3. Mobile device used as Point-of-Sale terminal must store all user-saved passwords in an encrypted password store.
4. Merchant must ensure that the password selected complies with the following password composition rules:
5. Password must be minimum eight alphanumeric characters long.
6. Password must have at least one lower case letter, one upper case letter, and one number.
7. Use special characters such as (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./) in password.
8. Password must not be a word in any language, slang, dialect, jargon, etc.
9. Passwords must not be based on personal information, names of family, friends, relations, colleagues, etc.
10. Regularly change the password.
11. Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user.
12. All passwords must be promptly changed if they are suspected of being disclosed or known to have been disclosed to unauthorized parties.

13. Passwords must not be written down and if they are, then the paper must be shredded after use or kept under lock.

13. SECURITY

1. The operating system of the mobile device used as Point-of-Sale terminal must be latest and up to date with patch cycles.
2. As a minimum patch must be checked weekly and applied at least once a month.
3. Mobile device used as Point-of-Sale terminal must not be "jailbroken" or "rooted" or have any software/firmware installed which is designed to gain full access to the root of the operating system.
4. Applications must only be installed from approved sources.

14. ANTI-VIRUS OR ANTI-MALWARE SOFTWARE PROGRAM

1. Regularly update anti-virus and anti-malware solution on the mobile device used as Point-of-Sale terminal.
2. Merchant must not delete, or disable, anti-virus or anti-malware software program, installed on mobile device used as Point-of-Sale terminal.
3. Regularly check for virus and malware using the virus and malware scanning software.
4. All incoming e-mails must be screened for viruses.
5. If you suspect infection by a virus or malware, immediately stop using the mobile device used as Point-of-Sale terminal.
6. Mobile device used as Point-of-Sale terminal must not be connected to a Personal Computer which does not have up to date and enabled anti-malware protection.

15. REPORTING OF INCIDENTS AND PROBLEMS

1. Merchant must allocate sufficient time to acquaint themselves with Bahrain's and regional Information Security and Privacy laws.
2. Any log-on problems, computer errors, security events or any observed or suspected security weaknesses in Eazy Point of Sale application must be reported to Eazy Financial Services as quickly as possible.
3. Merchant must report suspicious behaviour and indications of device tampering to Eazy Financial Services.
4. Eazy Financial Services reserves the right to revoke the privileges of any Merchant at any time. Conduct that interferes with the normal and proper operation of the application will not be permitted.

16. CONTACT US

Eazy welcomes your comments regarding this Privacy and Security Notice. If there is any concern related to processing of your personal data, please do not hesitate to reach out to our Data Protection Supervisor (DPS) through the below contact details:

DPS Email Address: DPS@eazy.net
Address: Eazy Financial Services B.S.C (Closed), Office 111, Building 709, Road 1708, Block 317, Diplomatic Area, P.O.BOX 75194 Manama - Kingdom of Bahrain

We will take commercially and reasonable efforts to promptly determine and remedy the problem.