PayU S.A.
186, Grunwaldzka Str.
60-166 Poznań
Poland

Tel. +48 61 628 45 05
Email: help@payu.pl
www.payu.pl

GUIDELINES ON SECURITY OF PAYMENT DATA PROCESSING

- This document contains a set of Partner's duties resulting from the use of Services provided by PayU with a Token.

- The capitalised terms not defined herein shall have the meaning defined in the Terms and Conditions of the System, Terms and Conditions of Pay by Payment Card Service, Terms and Conditions of Electronic Payment Service and the Agreement for Service Offering.

To improve the security of online payments, each Partner processing, storing or transmitting payment data should implement relevant security measures in IT systems. Payment data is understood as any tools used to make online payments, including without limitation Tokens representing payment instruments (such as cards). However, upon PayU request, Partners should explain and justify any cases of non-conformity of practice used in their operations.

Below you may find security mechanisms to be implemented by the Partner:

1. Management of access rights to IT systems:
   - Access to IT systems (server, firewall, network device, test and live environments, etc.) should result from employee duties and comply with the principle of granting only the required rights.
   - Relevant allocation of tasks in IT environments (e.g. development, test and live environments).
   - Each user should have his own login and access password meeting a relevant security level (recommended settings: at least 8 characters with 3 out of 4 parameters: capital letter, small letter, digit, special character).
2. Network and system security:
   - Transmission of sensitive payment data through the public network should be secured with secured transmission methods such as TLS (recommended protocols: TLS 1.1 or higher).
   - IT systems should be configured in accordance with good security practice such as NIST, SANS, etc.
3. Monitoring, security tests and audits
   - Access to critical IT resources (networks, databases, etc.) should be monitored and tracked.
   - IT systems should be subject to periodic security tests and audits to detect any threats, security gaps and vulnerabilities. Audits should be carried out by independent experts.

PayU SA with the registered Office in Poznań, 60-166 Poznań, ul. Grunwaldzka 186, entered into the Register of Entrepreneurs kept by the District Court for Poznań - Nowe Miasto and Wilda in Poznań, 8th Commercial Department of the National Court Register under KRS number 000027^399, with share Capital of PLN 0,9^,000 (paid up in full), tax identification number (NIP): 779-23-08-ir95, statistical number REGON 300523AAA.