PayU S.A.
ul. Grunwaldzka 186
60-166 Poznań

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

Payment Data Processing Security Guidelines

- *This document sets out the Partner's obligations in connection with the use of services provided by PayU using a Token.*

- *Terms written with a Capital Letter but not defined in this document shall have the meaning ascribed to them in the System Regulations, the Card Payment Service Regulations, the Electronic Payment Service Regulations, and the Service Provision Agreement.*

To increase the level of security of online payments, every Partner that processes, stores, or transmits payment data should implement appropriate security mechanisms in IT systems. By payment data, we mean all tools that can be used to make online payments, including Tokens representing payment instruments (e.g. cards). Upon PayU's request, Partners should explain and justify any instances of non-compliance with the practices used in their operations.

Below are the security mechanisms that the Partner should implement.

1. Systems Access Rights Management:
   - Access to IT systems (servers, firewalls, network devices, test and production environments, etc.) should be based on the employee's duties and comply with the principle of least privilege.
   - Appropriate segregation of duties in IT environments (e.g. development, test, and production environments).
   - Each user should have their own individual login and password meeting the appropriate security level (recommended settings: minimum password length of 8 characters, using at least 3 of the following: uppercase letter, lowercase letter, digit, special character).
2. Network and Systems Security:
   - The transmission of sensitive payment data over public networks should be secured using secure transmission methods, such as TLS (recommended protocols: TLS 1.2 + SNI or higher).
   - IT systems should be configured in accordance with security best practices, such as NIST, SANS, etc.
3. Monitoring, Security Testing, 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 for the detection of threats, vulnerabilities, and weaknesses. Audits should be conducted by independent experts.