PWE data protection

1. Confidentiality of IT systems and data processing

Measures suitable to prevent unauthorised access to data processing systems processing or utilising personal data

a) Building access control

The Paymentworld Group has two sites. They are:

- *Hamburg*
- *Malta*

The following measures have been taken:

- Access to the buildings only with special key and / or magnetic card. These are given to employees in person against a receipt

- All buildings have video surveillance and an alarm system

The data centre (looked after by Sentinel) covers the following measures:

- Personalised electronic access control systems: magnetic card and PIN

- The following are used: single access control systems, safety locks, door controls, window controls etc.

- Access rules for external persons, escorting of external visitors: by employees or contractor

- Monitoring equipment, through alarm systems and video surveillance

- Multiple access protection (access card, currently biometric characteristics, plus mechanical lock) for the data centre

The data centre has been certified in accordance with ISO2701 information security.

2. Reference to: Payment Card Industry (PCI)

Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire A
and Attestation of Compliance

We process this questionnaire every 3 months to enable an extension of the PCI certificate.

PWE is classified in accordance with PCI specification (the complete certificate is included in the appendix)

Since MasterCard requires our IT Systems to be PCI DSS Level 3 compliant, we are undergoing quarterly external PCI DSS Security Scans conducted by

usd AG
Frankfurter Str. 233, Haus C1
63263 Neu-Isenburg
Phone: +49 6102 8631 90
Fax: +49 6102 8631 88
E-Mail: contact@usd.de

There is a quarterly PCI - Compliance check / Scan for Paymentworld. The PCI certificate is renewed yearly.

Once a scan has been successfully passed usd AG issues a PCI Certificate that confirms that

PAYMENTWORLD EUROPE LIMITED ROC Company ID: C 65783 177, MARINA STREET, PTA 9072 PIETA' Malta

successfully provided evidence of compliance according to the Payment Card Industry Data Security Standard (PCI DSS) Version 3.2.

The current Self-Assessment Questionnaire (SAQ) has been renewed on 14.06.2017, now valid until **14.06.2018:**

2017-06-14-PCI-DSS-SAQ-PMW.pdf

usd AG also provides a Seal of Approval for our PWM website. The usd PCI DSS seal helps to demonstrate to our customers the security of our IT systems, which are accessable from the internet.

The english version can be found here: https://pci.usd.de/compliance/5890-D88D-D227-47A5-C541-641E/details_en.html

The german version can be found here: https://pci.usd.de/compliance/5890-D88D-D227-47A5-C541-641E/details_de.html

b) Access control

Examples:

1) BIP: (Paymentworld Payment Gateway)

PWE uses different systems to fulfil its payment obligation.

Non-personalised Payment Gateway
Due to compliance requirements PWE must check all login accounts regularly.
Part of this check is to ensure, that all accounts are still active and that there are NO active non-personalised login accounts like info@merchant-name.com.

2) Accounting System

The Microsoft Dynamics Client supports four credential authorisation mechanisms for Microsoft Dynamics users. When you create a user, you provide different information depending on the credential type that you are using in the current Microsoft Dynamics Server instance.

All users of a Microsoft Dynamics Server instance must be using the same credential type. You specify which credential type is used for a particular Microsoft Dynamics Server instance in the Microsoft Dynamics Server Administration tool.

The four credential types are:

Credential types	Description
Windows	With this credential type, users are authenticated using their Windows credentials. You can only specify Windows as the credential type if the corresponding user exists in Windows (Active Directory, local workgroup, or the local computer's users). Because they are authenticated through Windows, Windows users are not prompted for credentials when they access Microsoft Dynamics
UserName	With this setting, the user is prompted for username/password credentials when they access Microsoft Dynamics. These credentials are then validated against Windows authentication by Microsoft Dynamics Server. There must already be a corresponding user in Windows. Security certificates are required to protect the passing of credentials across a wide-

Credential types	Description
	area network. Typically, this setting should be used when the Microsoft Dynamics Server computer is part of an authenticating Active Directory domain, but the computer where the Microsoft Dynamics Windows client is installed is not part of the domain.
Password	With this setting, authentication is managed by Microsoft Dynamics Server but is not based on Windows users or Active Directory. The user is prompted for username/password credentials when they start the client. The credentials are then validated by an external mechanism. Security certificates are required to protect the passing of credentials. This mode is intended for hosted environments, for example, where Microsoft Dynamics is implemented in Azure.
AccessControlService	With this setting, Microsoft Dynamics relies on Microsoft Azure Access Control service (ACS) or Azure Active Directory (Azure AD) for user authentication services. ACS is a cloud service that provides user authentication and authorization for web applications and services. ACS integrates with standards-based identity providers, including enterprise directories such as Active Directory, and web identities such as Microsoft account, Google, Yahoo!, and Facebook. For more information, see Authenticating Users with Microsoft Azure Access Control Service. Azure AD is a cloud service that provides identity and access capabilities, such as for applications on Azure, in Microsoft Office 365, and for applications that install on-premises. If the Microsoft Dynamics Server instance is configured to use AccessControlService authentication, you can specify an Azure AD account for each user in the **Office 365 Authentication** field so that they can access both the Microsoft Dynamics Web client and their Office 365 site. Also, if you use Microsoft Dynamics in an app for SharePoint, users have single sign-on between the SharePoint site and Microsoft Dynamics. For more information, see Authenticating Users with Azure Active Directory.

Basic IT Guidelines for Paymentworld

1. Shutdown your Laptop/PC at the end of every day or **reboot** it at the beginning of **every** working day.

2. If you experience any "problem" **reboot** your Laptop/PC **first** and check if your problem is solved now **before** contacting IT.
3. **Always** use your **LAN cable** to connect to the company network. The WIFI may only be used when the internal network is not working. So consider the WIFI as emergency fallback.
4. Always use **Chrome** as your **standard browser** and allow it to update when asked.
5. Do not install any third party software on your own. Consult with IT if you need anything to be installed.
6. Keep your Java updated. Whenever Java is asking for an update please run the update.
7. Change your passwords on a regular base.
8. Do not share password between staff.

c) Access control (access rights)

1. BIP: Payment Gateway

Paymentworld uses an International Payment Gateway. The Gateway has a dedicated user right per role concept:

d) Separation control

Paymentworld uses suitable measures to ensure that data collected for different purposes are processed separately.

For example data from production and from the test operation of the operative system are kept on different data servers.

Reference to:

Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire A
and Attestation of Compliance

e) Pseudonymisation

Currently no information

2. Integrity of IT systems and data processing

a) Forwarding control

PWE utilises common industry standards to guarantee the prevention of unauthorised reading, copying, modification or removal of personal data during their electronic transmission or transport or storage on data carriers.

The related PWE measures include:

- Use of VPN (Virtual Private Networks)

- Setup and regular review of the firewalls used
- Use of antivirus programs in the applications

b) Input control

Corresponding LOG files are generated and subsequently reviewed for suspected abuse.

-> LogFiles are included (Accounting ERP)
-> Payment-Gateway(s) of Paymentworld

3. Availability, capacity and speedy recoverability of the IT systems and data processing

-> Distribution over various data centres
-> Business-critical applications, such as KontoCloud, ACI PayOn Gateway

-> Data Hosting / Storage: https://sentinel-it.de

-> Back-up procedures

-> Firewall protection (provider)

The following companies provide the business-critical applications for Paymentworld:

https://www.aciworldwide.com
https://contoworks.com
https://www.unicreditgroup.eu/en.html

4. Procedures for regular review, assessment and evaluation

Paymentworld regularly applies procedures and measures suitable to ensure that the effectiveness of the technical and organisational measures for guaranteeing data and IT security are regularly reviewed, assessed and evaluated.

Reference is made to the regular PCI audit by the firm usd (Frankfurt/M.)

5. Data Protection Officer (DPO)

Data Controller	
Name & Surname of DPO	**Daniela Grioli**
Position	**Head of Operations**
Mailing Address	**Skyway Offices Block A Suite 3**
	177 Marina Street, Pieta PTA 9072
Email Address	grioli@paymentworld.eu
Contact Number	**27781395**
Nature of Business	**Electronic Money Institution**
Date of Appointment	**25 May 2018**
Designated for other Data Controllers	**N/A**