PWE - Datenschutzhinweise

1. Vertraulichkeit der IT -Systeme und Datenverarbeitung

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen *personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren*

a) Zutrittskontrolle Gebäude

Die Paymentworld - Gruppe verfügt über zwei Standorte. Diese sind:

- *Hamburg*
- *Malta*

Folgende Maßnahmen wurden getroffen:

- Zutritt zu den Gebäuden nur mit speziellem Schlüssel und / oder Magnetkarte. Die Übergabe erfolgt an den Mitarbeiter / Mitarbeiterin persönlich mit Empfangsquittung

- Alle Gebäude sind Video-überwacht und besitzen eine Alarmanlage

Das Rechenzentrum (betreut von der Firma Sentinel) umfasst folgende Maßnahmen:

- Personalisierte elektronisches Zutrittskontrollsysteme: Magnetkarte und PIN

- Eingesetzt werden: Vereinzelungsanlagen, Sicherheitsschlösser, Türsicherungen, Fenstersicherungen etc.

- Zutrittsregelegungen für externe Personen; Begleitung betriebsfremder Personen durch Mitarbeiter oder den Auftragnehmer

- Überwachungseinrichtungen, durch Alarmanlagen und Videoüberwachung

- Mehrfach-Zutrittsschutz (Zutrittskarte, zzgl. biometrischem Merkmal, zzgl. mechanischem Schloss) für das Rechenzentrum

Das Rechenzentrum ist nach ISO27001 Informationssicherheit zertifiziert.

2. Verweis auf: Payment Card Industry (PCI)

Payment Card Industry (PCI)
Datensicherheitsstandard (Data Security Standard)
Fragebogen A zur Selbsteinschätzung (Self-Assessment Questionnaire A)
und Bescheinigung der Erfüllung

Dieser Fragebogen wird von uns jeweils alle 3 Monate bearbeitet und ermöglicht die Verlängerung des PCI Zertifikates.

PWE ist nach PCI Vorgabe klassifiziert (Anhang erhält das vollständige Zertifikat)

Seit MasterCard fordert, dass unsere IT-Systeme mit dem PCI DSS Level 3 konform sind, unterziehen wir uns vierteljährlichen externen PCI DSS Sicherheitsscans, die durch die

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

durchgeführt werden.

Es gibt vierteljährliche PCI – Konformitätschecks / Scans für Paymentworld. Das PCI-Zertifikat wird jährlich erneut.

Sobald ein Scan erfolgreich durchgeführt wurde, erteilt die usd AG ein PCI-Zertifikat, das bestätigt, dass die

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

erfolgreich den Nachweis der Konformität gemäß den Payment Card Industry Data Security Standard (PCI DSS) Version 3.2 erbracht hat.

Der aktuelle Fragebogen zur Selbstveranlagung wurde am 14.06.2017 erneuert und ist nunmehr bis zum **14.06.2018** gültig:

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

Die usd AG stellt zudem ein Gütesiegel für unsere PWM Internetseite zur Verfügung. Das usd PCI DSS Siegel unterstützt dabei, unseren Kunden die Sicherheit unserer IT-Systeme, die über das Internet zugänglich sind, darzulegen.

Die englische Version findet sich hier: https://pci.usd.de/compliance/5890-D88D-D227-47A5-C541-641E/details_en.html

Die deutsche Version findet sich hier: https://pci.usd.de/compliance/5890-D88D-D227-47A5-C541-641E/details_de.html

b) Zugangskontrolle

Beispiele:

1) BIP: (Paymentworld Payment Gateway)

PWE nutzt verschiedene Systeme um ihre Zahlungsverpflichtung zu erfüllen.

Das nicht-personalisierte Zahlungsportal
Aufgrund von Compliance-Anforderungen muss PWE alle Benutzerkonten regelmäßig prüfen.
Teil dieser Prüfung ist sicherzustellen, dass alle Konten noch immer aktiv sind und dass keine NICHT aktiven nicht-personalisierten Benutzerkonten wie info@merchant-name.com vorhanden sind.

2) Abrechnungssystem

Der Microsoft Dynamics Client unterstützt vier Berechtigungsnachweis-Authorisierungsmechanismen für den Microsoft Dynamics-Nutzer. Wenn man einen Nutzer anlegt, stellt man verschiedene Informationen zur Verfügung, abhängig von dem Typ des Berechtigungsnachweises, den man in der aktuellen Microsoft Dynamics Server-Instanz nutzt.

Sämtliche Nutzer einer Microsoft Dynamics Serverinstanz müssen denselben Typ eines Berechtigungsnachweises nutzen. Im Microsoft Dynamics Server Administrations Tool legt man fest, welcher Berechtigungsnachweistyp für eine bestimmte Microsoft Dynamics Server-Instanz genutzt wird.

Die vier Berechtigungsnachweis-Typen sind:

Berechtigungsnachweistyp	Beschreibung
Windows	Mit diesem Berechtigungsnachweistyp wird der Nutzer mittel seiner Windows Anmeldedaten authentifiziert. Man kann Windows nur als Berechtigungsnachweistyp festlegen, wenn der entsprechende Nutzer in Windows existiert (Active Directory, lokale Arbeitsgruppe, oder der lokale Computernutzer). Weil sie über Windows authentifiziert werden, werden Windows-Nutzer nicht aufgefordert, Anmeldedaten einzugeben, wenn sie auf Microsoft

Berechtigungsnachweistyp	Beschreibung
	Dynamics zugreifen.
Benutzername	Mit dieser Einstellung wird der Benutzer aufgefordert, die Anmeldeinformationen Benutzernamen/Passwort einzugeben, wenn sie auf Microsoft Dynamics zugreifen. Diese Anmeldedaten werden gegenüber der Windows-Authentifizierung durch den Microsoft Dynamics Server bestätigt. Ein entsprechender Nutzer muss in Windows bereits vorhanden sein. Sicherheitszertifikate sind erforderlich um das Weiterleiten von Anmeldedaten über öffentliche Netze (wide-area network) zu schützen. Typischerweise sollte diese Einstellung genutzt werden, wenn ein Microsoft Dynamics Server Computer Teil einer authentifizierten Active Directory Domain ist, jedoch der Computer, der auf dem Microsoft Dynamics Windows Client installiert ist, kein Teil der Domain ist.
Passwort	Mit dieser Einstellung wird die Authentifizierung von dem Microsoft Dynamics Server verwaltet, basiert aber nicht auf Windows-Nutzern oder Active Directory. Der Nutzer ist aufgefordert die Anmeldedaten Benutzername/Passwort einzugeben, wenn er den Client startet. Die Anmeldedaten werden dann durch einen externen Mechanismus bestätigt. Sicherheitszertifikate sind erforderlich, um die Weiterleitung der Anmeldedaten zu schützen. Diese Art ist für gehostete Umgebungen vorgesehen, z.B. wenn Microsoft Dynamics in Azure eingebunden ist.
Zugriffskontrolldienste	Mit dieser Einstellung setzt Microsoft Dynamics für Nutzer Authentifizierungsdienste auf Microsoft Azure Access Control Service (ACS) oder Azure Active-Directory (Azure AD) auf. ACS ist ein Cloud-Service, der eine Nutzerauthentifizierung und die Authentifizierung für Webanwendungen und Dienstleistungen zur Verfügung stellt. ACS bindet standardbasierte Identity-Provider ein, einschließlich Unternehmensverzeichnissen wie Active-Directory, und Web-Identitäten wie ein Microsoft-Konto, Google, Yahoo! und Facebook. Für mehr Informationen siehe Authenticating Users with Microsoft Azure Access Control Service. Azure AD ist ein Cloud-Service, der Identitäts- und Zugriffsmöglichkeiten zur Verfügung stellt, wie die

Berechtigungsnachweistyp	Beschreibung
	Anwendugnen auf Azure, in Microsoft Office 365 und für Anwendungen, die on-premises installieren. Soweit die Microsoft Dynamics Server-Instanz konfiguriert ist, um die zur Authentifizierung Zugangskontrolldienste zu nutzen, kann man für jeden Nutzer ein Azure AD-Konto im Office 365 Authentifizierungsfeld festlegen, so dass diese sowohl auf den Microsoft Dynamics Web Client als auch deren Office 365-Seite Zugriff haben. Wenn man Microsoft Dynamics als App für SharePoint nutzt, haben Nutzer zudem eine Einzelanmeldung zwischen der SharePoint-Seite und Microsoft Dynamics. Für mehr Informationen siehe Authenticating Users with Azure Active Directory.

Grundlegende IT-Richtlinien für Paymentworld

1. Fahren Sie Ihren Laptop/PC am Ende jedes Tages runter und starten Sie ihn am Beginn jedes Arbeitstages neu.
2. Wenn Sie irgendein „Problem“ feststellen, starten Sie Ihren Laptop/PC zunächst neu und prüfen, ob das Problem gelöst ist, bevor Sie die IT kontaktieren.
3. Nutzen Sie immer das LAN-Kabel um sich mit dem Unternehmensnetzwerk zu verbinden. WIFI sollte nur genutzt werden, wenn das interne Netzwerk nicht funktioniert. Betrachten Sie daher das WIFI als Notfalllösung.
4. Nutzen Sie immer Chrome als Standardbrowser und gestatten Sie ein Update, wenn Sie dazu aufgefordert werden.
5. Installieren Sie nicht selbstständig Software von Dritten. Ziehen Sie die IT hinzu, wenn Sie etwas installieren wollen.
6. Halten Sie Java auf dem neuesten Stand. Wenn Java ein Update anfragt, führen Sie das Update durch.
7. Ändern Sie Ihr Passwort auf regelmäßiger Basis.
8. Teilen Sie Ihr Passwort nicht mit Mitarbeitern.

c) Zugriffskontrolle (Zugriffsrechte)

BIP: Zahlungsportal

Paymentworld nutzt ein internationales Zahlungsportal. Das Portal hat ein dezidiertes Konzept der Nutzer je Rolle.

d) Trennungskontrolle

Paymentworld setzt geeignete Maßnahmen ein, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Beispielsweise werden Daten der Produktion und des Test-Betriebes der operativen Systeme auf unterschiedlichen Daten-Servern gehalten.

Verweis auf:

Payment Card Industry (PCI)
Datensicherheitsstandard (Data Security Standard)
Fragebogen A zur Selbsteinschätzung (Self-Assessment Questionnaire A)
und Bescheinigung der Erfüllung

e) Pseudonymisierung

derzeit keine Angaben

2. Integrität der IT-Systeme und Datenverarbeitung

a) Weitergabekontrolle

PWE nutzt die gängigen Industriestandards um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Maßnahmen der PWE umfassen hierzu:

- Nutzung des VPN (Virtual Private Networks)
- Etablierung und regelmäßige Prüfung der eingesetzten Firewalls
- Verwendung von Virenschutzprogrammen in den Applikationen

b) Eingabekontrolle

Es werden entsprechende LOG-Dateien generiert und nachträglich bei Verdacht auf Missbrauch überprüft.

-> LogFiles werden mitgeschrieben (Accounting ERP)
-> Payment-Gateway(s) der Paymentworld

3. Verfügbarkeit, Belastbarkeit und rasche Wiederherstellbarkeit der IT-Systeme und Datenverarbeitung

-> Verteilung auf verschiedene Rechenzentren
-> Geschäftskritische Anwendungen wie z.B. KontoCloud, ACI PayOn Gateway

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

(c) Paymentworld

-> Back up Verfahren

-> Firewall - Schutz (Anbieter)

Folgende Unternehmen stellen die geschäftskritischen Applikationen für die Paymentworld zur Verfügung:

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

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Paymentworld unterzieht sich regelmäßigen Verfahren und Maßnahmen, die geeignet sind zu gewährleisten, dass die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Sicherstellung der Daten- und IT Sicherheit regelmäßig überprüft, bewertet und evaluiert werden.

Das regelmäßige PCI-Audit wird von der Firma usd, Frankfurt/M. durchgeführt

5. Datenschutzbeauftragter

Vorname und Name	**Daniela Grioli**
Position	**Head of Operations**
Adresse	**Skyway Offices Block A Suite 3**
	177 Marina Street, Pieta PTA 9072
Email	grioli@paymentworld.eu
Kontakt-Nummer	**27781395**
Art der Geschäftstätigkeit	E-Geld Institut
Datum der Bestimmung	**25. Mai 2018**
Vorgesehen für andere Datenverarbeiter	**N/A**