



# **Payment Card Industry Data Security Standard**

---

## **Attestation of Compliance for Report on Compliance – Service Providers**

**Version 4.0.1**

Publication Date: August 2024



# **PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: Worldline eCommerce Solutions BVBA / SPRL**

**Date of Report as noted in the Report on Compliance: 18 Jan 2026**

**Date Assessment Ended: 18 Jan 2026**



## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* ("Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

### Part 1. Contact Information

#### Part 1a. Assessed Entity (ROC Section 1.1)

Company name:	Worldline eCommerce Solutions BVBA / SPRL
DBA (doing business as):	-
Company mailing address:	Chau. de Haecht 1442, 1130 Brussels, Belgium
Company main website:	<a href="https://www.worldline.com/">https://www.worldline.com/</a>
Company contact name:	Geert Van De Wielle
Company contact title:	Chief Information Security Officer
Contact phone number:	+32 2 727 61 11
Contact e-mail address:	<a href="mailto:geert.vandewielle@worldline.com">geert.vandewielle@worldline.com</a>

#### Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)	
ISA name(s):	N/A
Qualified Security Assessor	
Company name:	usd AG
Company mailing address:	Frankfurter Str. 233, Haus C1, 63263 Neu-Isenburg, Germany
Company website:	<a href="https://www.usd.de">https://www.usd.de</a>
Lead Assessor name:	Julia Wingert
Assessor phone number:	+49 6102 8631 336
Assessor e-mail address:	<a href="mailto:julia.wingert@usd.de">julia.wingert@usd.de</a>
Assessor certificate number:	QSA (205-438)



## Part 2. Executive Summary

### Part 2a. Scope Verification

Services that were **INCLUDED** in the scope of the Assessment (select all that apply):

Name of service(s) assessed:		Payment Processing, Payment Gateway/Switch, Clearing and Settlement, Fraud and Chargeback, Merchant Services	
Type of service(s) assessed:			
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input type="checkbox"/> POI / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):	
<input type="checkbox"/> Account Management	<input checked="" type="checkbox"/> Fraud and Chargeback	<input checked="" type="checkbox"/> Payment Gateway/Switch	
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services	
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management	
<input checked="" type="checkbox"/> Clearing and Settlement	<input checked="" type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments	
<input type="checkbox"/> Network Provider			
<input type="checkbox"/> Others (specify):			

**Note:** These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.



**Part 2. Executive Summary (continued)**

**Part 2a. Scope Verification (continued)**

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):**

Name of service(s) not assessed: -

Type of service(s) not assessed:

<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		

Provide a brief explanation why any checked services were not included in the Assessment:

N/A

**Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)**

Describe how the business stores, processes, and/or transmits account data.

Worldline eCommerce accepts Visa, MasterCard, American Express, Diners and JCB payment cards. Card-not-present payment channel and Payment gateway:  
 Cardholder data (PAN, cardholder name, expiry, card security codes (CVV2, CVC2, CID, CAV2)) is received from merchants and/or clients (white-labelled Payment Service Providers) via API integrations or from the cardholder via payment pages over TLS v1.2.  
 Authorization of transactions may be performed in real-time by the above or via a batch file (PAN, cardholder



	<p>name, expiry, card security codes (CVV2, CVC2, CID, CAV2)) received from the merchant / client. The batch file data flow is via a dedicated IPsec VPN (AES 256 and SHA256).</p> <p>The Front-end servers receive cardholder data (PAN, cardholder name, expiry, card security codes (CVV2, CVC2, CID, CAV2)) and make an API call to the Back-end servers.</p> <p>The Back-end servers are responsible for authorizing the transaction with the acquiring bank as well as updating the database historical record with cardholder data (PAN).</p> <p>The Back-end servers encrypt the cardholder data (PAN and card security codes (CVV2, CVC2, CID, CAV2)) and stores them in the Back-end MS SQL database encrypted (AES 256) prior to authorization. Upon completion of authorization processing a copy of cardholder data (PAN) is stored encrypted (AES 256), truncated (first 6 and last 4) and hashed while the originally stored data is destroyed encrypted using the databases inherent delete functions.</p> <p>Settlements transactions are retrieved from the Back-end MS SQL database by the Back-end Servers which transmits the transactions to the relevant acquirer over TLS v1.2.</p>
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>N/A</p>
<p>Describe system components that could impact the security of account data.</p>	<p>The payment applications used to capture consumer cardholder data, as well as the databases provided by Worldline SA in which cardholder data is stored could impact the security of account data.</p>



**Part 2. Executive Summary (continued)**

**Part 2c. Description of Payment Card Environment**

Provide a high-level description of the environment covered by this Assessment.

*For example:*

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*
- *System components that could impact the security of account data.*

Worldline eCommerce Solutions BVBA / SPRL (Worldline eCommerce) is a Level 1 Payment Service Provider.

Worldline eCommerce receives, transmits, and processes cardholder data (PAN, Cardholder name, expiry date, card security codes (CVV2, CVC2, CID, CAV2)) as part of its services.

Cardholder data (PAN, Cardholder name, expiry date, card security codes (CVV2, CVC2, CID, CAV2)) is received from merchants and/or clients (white-label Payment Service Providers) via API integrations or from the cardholder via payment pages over TLS v1.2.

Authorization transactions are either performed in real time or via batch files received from the merchant/client. The batch file data flow works via dedicated IPsec VPN.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment.

(Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)

Yes  No

**Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)**

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Corporate Office	1	Brussels, Belgium
Data Center	1	Equinix PA3 (114 Rue Ambroise Croizat, 93200 Saint-Denis, France)
Data Center	1	Telehouse 3 (1 Rue Pablo Picasso, 78114 Magny-les-Hameaux, France)
Data Center	1	Seclin data center (2 rue Marcel Dassault, Room SA 59113 Seclin Nord – France)



**Part 2. Executive Summary (continued)**

**Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)**

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions.\*?

Yes  No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
None	-	-	-	-

\* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.



**Part 2. Executive Summary (continued)**

**Part 2f. Third-Party Service Providers  
(ROC Section 4.4)**

For the services being validated, does the entity have relationships with one or more third-party service providers that:

<ul style="list-style-type: none"> <li>• Store, process, or transmit account data on the entity’s behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>• Manage system components included in the entity’s Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>• Could impact the security of the entity’s CDE (for example, vendors providing support via remote access, and/or bespoke software developers).</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

**If Yes:**

<b>Name of Service Provider:</b>	<b>Description of Services Provided:</b>
Worldline acceptance (Shared Services)	Several payment related services, including: Dynamic Currency Conversion HUB, United 3DS, Scheme Tokenization Shared Service, Global Tokenization Service, Acquirer Hub, Global HSM
Worldline SA (Central Hosting Provider)	Housing, Hosting, System Security Services, IT Support, Network Provider, Infrastructure Service, Backup and Storage, File Transfer Service, CaaS Platform, IaaS Platform, HSM and Key Management Services, Risk Management, Vulnerability Management, Security Incident Management, HR Management, Security Awareness Training, Secure Coding Training, Service Provider Management, Media Handling, Robotic Process Automation, SARA Advanced Infrastructure Services: Private Cloud Services, iRing Cyber Defense Center: Vulnerability Scanning, Penetration Testing, Log File Collection, Monitoring and Alerting, EDR

**Note:** Requirement 12.8 applies to all entities in this list.



**Part 2. Executive Summary (continued)**

**Part 2g. Summary of Assessment (ROC Section 1.8.1)**

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

**Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

*Name of Service Assessed:* Payment Processing, Payment Gateway/Switch, Clearing and Settlement, Fraud and Chargeback, Merchant Services

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Justification for Approach**



<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>2.3.1, 2.3.2, 4.2.1.2: No wireless networks are in scope of this assessment.                  3.3.3: The entity is not an issuer or a company that supports issuing services.                  3.5.1.2, 3.5.1.3: Disk-level or partition-level encryption is not used.                  3.6.1.3, 3.7.6, 3.7.8: No access to cleartext cryptographic key components.                  3.7.9: Worldline eCommerce never shares cryptographic keys with its customers.                  4.2.2: Worldline ecommerce never sends PANs via end-user messaging technologies.                  6.4.1, 8.3.10, 10.7.1: Requirements have been superseded after 31 Mar 2025.                  8.2.3: No remote access to customer premises.                  8.2.7: No accounts used by third parties.                  8.3.9: Passwords are never used as the only authentication factor.                  9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3, A2: No POS devices are in scope of this assessment.                  11.4.7, A1: Assessed entity is not a multi-tenant service provider.                  12.3.2: The entity does not use the customized approach.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>-</p>



## Section 2 Report on Compliance

**(ROC Sections 1.2 and 1.3)**

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>	16 Jul 2025
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	18 Jan 2026
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No



## Section 3 Validation and Attestation Details

### Part 3. PCI DSS Validation (ROC Section 1.7)

**This AOC is based on results noted in the ROC dated 18 Jan 2026.**

Indicate below whether a full or partial PCI DSS assessment was completed:

- Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.
- Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (*select one*):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall <b>COMPLIANT</b> rating; thereby Worldline eCommerce Solutions BVBA / SPRL has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall <b>NON-COMPLIANT</b> rating; thereby (<i>Service Provider Company Name</i>) has not demonstrated compliance with PCI DSS requirements.</p> <p><b>Target Date</b> for Compliance: YYYY-MM-DD</p> <p>An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.</p>								
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall <b>COMPLIANT BUT WITH LEGAL EXCEPTION</b> rating; thereby (<i>Service Provider Company Name</i>) has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								



### Part 3. PCI DSS Validation (continued)

#### Part 3a. Service Provider Acknowledgement

**Signatory(s) confirms:**

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

#### Part 3b. Service Provider Attestation

Signed by:  <small>C37A810CD86148F...</small>	
Signature of Service Provider Executive Officer ↑	Date: 18 January 2026   10:06 CET
Service Provider Executive Officer Name: <b>Geert Van de Wille</b>	Title: <b>Head of MS Security / CISO</b>


#### Part 3c. Qualified Security Assessor (QSA) Acknowledgement

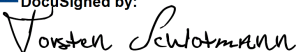
If a QSA was involved or assisted with this Assessment, indicate the role performed:

QSA performed testing procedures.

QSA provided other assistance.

If selected, describe all role(s) performed:

DocuSigned by:  <small>CA2C59095EED49B...</small>	
Signature of Lead QSA ↑	Date: 19 January 2026   07:06 CET
Lead QSA Name: <b>Julia Wingert</b>	

DocuSigned by:  <small>9366AA034EE04CE...</small>	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 18 January 2026   14:11 MEZ
Duly Authorized Officer Name: <b>Torsten Schlotmann</b>	QSA Company: <b>usd AG</b>

#### Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:

ISA(s) performed testing procedures.

ISA(s) provided other assistance.

If selected, describe all role(s) performed:



## Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input type="checkbox"/>	<input type="checkbox"/>	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: [https://www.pcisecuritystandards.org/about\\_us/](https://www.pcisecuritystandards.org/about_us/)

## Certificate Of Completion

Envelope Id: 98361D48-C718-4618-8DC4-961B75CF37A9  
 Subject: Complete with Docusign: PCI-DSS-v4-0-1-AOC\_023\_usd AG\_Wordline eComm.pdf  
 Source Envelope:  
 Document Pages: 15  
 Certificate Pages: 5  
 AutoNav: Enabled  
 Envelopeld Stamping: Enabled  
 Time Zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Status: Completed  
 Envelope Originator:  
 Nico Kemp  
 Frankfurter Str. 233, Haus C1  
 Neu-Isenburg, Hessen 63263  
 Nico.Kemp@usd.de  
 IP Address: 79.227.223.185

## Record Tracking

Status: Original  
 1/16/2026 1:55:23 PM  
 Holder: Nico Kemp  
 Nico.Kemp@usd.de  
 Location: DocuSign

## Signer Events

Geert Van De Wille  
 geert.vandewille@worldline.com  
 CISO Worldline nv/sa  
 Security Level: Email, Account Authentication (None)

## Signature

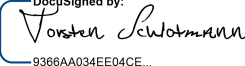
Signed by:  
  
 C37A810CD86148F...  
 Signature Adoption: Pre-selected Style  
 Using IP Address:  
 2a02:1812:2407:c200:d5a2:a619:6c4d:8ba8  
 Signed using mobile

## Timestamp

Sent: 1/18/2026 10:00:08 AM  
 Viewed: 1/18/2026 10:05:47 AM  
 Signed: 1/18/2026 10:06:23 AM

**Electronic Record and Signature Disclosure:**  
 Accepted: 1/18/2026 10:05:47 AM  
 ID: 56f4bddd-c589-4f3b-8154-a93ca02be11b

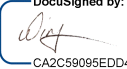
Torsten Schlotmann  
 torsten.schlotmann@usd.de  
 usd AG  
 Security Level: Email, Account Authentication (None)

DocuSigned by:  
  
 9366AA034EE04CE...  
 Signature Adoption: Pre-selected Style  
 Using IP Address:  
 2a0a:a54b:a7f:0:ddb3:8152:197f:1d2e  
 Signed using mobile

Sent: 1/18/2026 10:06:25 AM  
 Viewed: 1/18/2026 2:11:11 PM  
 Signed: 1/18/2026 2:11:57 PM

**Electronic Record and Signature Disclosure:**  
 Not Offered via Docusign

Julia Wingert  
 julia.wingert@usd.de  
 usd AG  
 Security Level: Email, Account Authentication (None)

DocuSigned by:  
  
 CA2C59095EDD49B...  
 Signature Adoption: Uploaded Signature Image  
 Using IP Address: 87.78.45.225  
 Signed using mobile

Sent: 1/18/2026 2:12:00 PM  
 Viewed: 1/19/2026 7:06:29 AM  
 Signed: 1/19/2026 7:06:36 AM

**Electronic Record and Signature Disclosure:**  
 Not Offered via Docusign

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp

<b>Carbon Copy Events</b>	<b>Status</b>	<b>Timestamp</b>
---------------------------	---------------	------------------

<b>Witness Events</b>	<b>Signature</b>	<b>Timestamp</b>
-----------------------	------------------	------------------

<b>Notary Events</b>	<b>Signature</b>	<b>Timestamp</b>
----------------------	------------------	------------------

<b>Envelope Summary Events</b>	<b>Status</b>	<b>Timestamps</b>
--------------------------------	---------------	-------------------

Envelope Sent	Hashed/Encrypted	1/18/2026 10:00:08 AM
Certified Delivered	Security Checked	1/19/2026 7:06:29 AM
Signing Complete	Security Checked	1/19/2026 7:06:36 AM
Completed	Security Checked	1/19/2026 7:06:36 AM

<b>Payment Events</b>	<b>Status</b>	<b>Timestamps</b>
-----------------------	---------------	-------------------

<b>Electronic Record and Signature Disclosure</b>
---

## **CONSUMER DISCLOSURE**

From time to time, usd AG (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign, Inc. (DocuSign) electronic signing system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the 'I agree' button at the bottom of this document.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after signing session and, if you elect to create a DocuSign signer account, you may access them for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign 'Withdraw Consent' form on the signing page of a DocuSign envelope instead of signing it. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures

electronically from us.

**How to contact usd AG:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: [lorenz.heiler@usd.de](mailto:lorenz.heiler@usd.de)

**To advise usd AG of your new e-mail address**

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at [lorenz.heiler@usd.de](mailto:lorenz.heiler@usd.de) and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc. to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in the DocuSign system.

**To request paper copies from usd AG**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to [lorenz.heiler@usd.de](mailto:lorenz.heiler@usd.de) and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

**To withdraw your consent with usd AG**

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your DocuSign session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an e-mail to [lorenz.heiler@usd.de](mailto:lorenz.heiler@usd.de) and in the body of such request you must state your e-mail, full name, US Postal Address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

**Required hardware and software**

Operating Systems:	Windows® 2000, Windows® XP, Windows Vista®; Mac OS® X
Browsers:	Final release versions of Internet Explorer® 6.0 or above (Windows only); Mozilla Firefox 2.0 or above (Windows and Mac); Safari™ 3.0 or above (Mac only)
PDF Reader:	Acrobat® or similar software may be required to view and print PDF files
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	Allow per session cookies

\*\* These minimum requirements are subject to change. If these requirements change, you will be asked to re-accept the disclosure. Pre-release (e.g. beta) versions of operating systems and browsers are not supported.

**Acknowledging your access and consent to receive materials electronically**

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the 'I agree' button below.

By checking the 'I agree' box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC CONSUMER DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify usd AG as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by usd AG during the course of my relationship with you.