Version April 2025

Frequently Asked Questions

Welcome to our FAQs on Data Protection, Cloud Security, and GDPR. This quick guide helps you to understand whether and how we process your data, especially concerning cloud security (SaaS).

Part 1 – General Information		
#	Question	Response
General		
	Vendor/Provider Name	PTM EDV Systeme GmbH
	Vendor/Provider Website	www.ptm-edv.at
	Product Websites	www.mscrm-addons.com www.poweraddons.com
	Registered Office	Bahnhofguertel 59 8020 Graz Austria
	Legal Documents (General T&C, Data Processing Contract)	https://www.mscrm-addons.com/LegalDocuments
	Support Terms and Conditions	https://www.mscrm-addons.com/language/en-US/Support/Terms-Conditions
	Data Protection Officer (external)	Karl Pusch (DPO Consult GmbH)
	Data Protection Coordinator (internal)	Julian Handl, Office & ISMS Manager gdpr@ptm-edv.at
	Certifications	1. Since April 2024 PTM EDV Systeme GmbH has been **ISO27001:2022** certified. For further details, please see the first section below. The certificate will be provided upon request. 2. We participate in the **Microsoft 365 App Compliance Program** and hold a Publisher Verification. Our Add-Ons are available on Microsoft AppSource and have undergone the AppSource certification process. 3. An external gray-box **Penetration Test** was performed on the website, service configuration, and Azure infrastructure of http://mscrm-addons.com, in compliance with OWASP Top 10 standards. The most recent certification can be found here.
ISO27001		

	Scope	All products, departments, employees, services, and infrastructure of PTM EDV Systeme GmbH are fully covered by the ISMS. This includes all websites and online services operated under www.ptm-edv.at, www.mscrm-addons.com, and www.poweraddons.com.
	ISMS Team & competences	• Christian Ternek CEO & Head of the ISMS • Julian Handl Office & certified ISMS Manager • Patrick Leitner IT-System Administrator & certified ISMS Manager
	ISMS Management	To ensure an even higher standard of our ISMS, we work together with the external consulting and ISMS management company SecFix GmbH.
	Covered and implemented topics of relevance	• Risk Management • Access Management • Vendor Management • Asset Management • Vulnerability Management • Business Continuity and Disaster Recovery Plans • Incident Response Plan • Cloud Security • Secure Development
	Policy Overview	See Appendix 01
Organizational security		
	Do you offer technical and organizational measures according to Art. 32 GDPR?	Yes, you can review them by clicking below: ➔ TOMs - PTM EDV Systeme
	Purpose of these TOMs	These TOMs describe the measures of our internal systems where we process general business data such as invoices required for business transactions with you. **No data processed with our products, either by you or your customers, is processed locally on our side!**
	Do you ensure compliance with information security laws and, if so, how?	We work with an external data privacy company (incl. external DPO) and have a certified internal Data Protection Coordinator. GDPR compliance is a core requirement of our ISO 27001-certified ISMS.

	Has a formal Information Security Policy been implemented?	Yes, all employees are aware of the data protection declaration and have signed the IT security policy.
	How do you ensure that all employees are aware of the most important cyber security issues?	Every employee has to complete comprehensive online training at least once a year.
	Does your organization enforce a strong password policy?	Yes, passwords must contain at least 10 characters, including 8 alphanumeric characters, upper and lower case letters, one number, and one special character. Passwords must be securely managed with KeePass.
	Regarding the Software, please describe your patch management process	1. Issue Reporting: Customer-reported issues or internal testing identify issues. 2. Issue Reproduction/Analysis: Reported issues are thoroughly reproduced and analyzed. 3. Fix or Workaround Implementation: Fixes or workarounds are implemented. 4. Testing: Comprehensive testing is conducted, including automated and manual testing. 5. Release: The fixed and tested solution is released to ensure availability to users. Comment: Standard issues under our control are typically resolved within a few days after reproduction and analysis. Critical fixes are promptly released. Fortunately, we haven't experienced any critical incidents to date.
Physical security		
	Do you apply physical security measures to information security, and if so, to what extent (zone and room security)?	The office and every entrance are monitored with video surveillance cameras. The reception has full overview of every person entering or exiting the company office. The server room is secured with a smart lock, permitting entry only to authorized personnel, with every access logged.
	Do you apply environmental security measures to information security, and if so, which and to what extent (server room tele-technical systems)?	The server room is equipped with a temperature and humidity measuring device that alerts the IT Department and CEO of any temperature changes.
	Please see our TOMs for further physical security measures	
IT security		
	Has the formal process of granting rights and changes to IT systems been introduced?	Yes, rights and change management are handled exclusively by our IT administration in accordance with the ISO 27001 requirements for Access and

		Change Management. For automated processes, designated technical service accounts are used.
	Do you apply cryptographic security measures and if so, to what extent?	Yes, cryptographic security measures are employed on the hard disks (PCs & Laptops) to prevent data loss in case of stolen company devices. Additionally, the VPN connection is encrypted with SSL.
	Have you defined IT operational procedures for managing change, performance and separation of environments?	Yes, the IT department oversees change, performance, and separation of environments. Changes undergo testing beforehand, and data is backed up before any change, which can be applied for restoring the testing & operational systems.
	Do you have a Backup Policy and if so, what does it include?	We have a detailed Backup and Recovery Policy in place. All company servers and critical systems are regularly backed up according to defined schedules and the criticality of the data.
	How do you ensure protection against malware?	Company devices are safeguarded against malware with antivirus software automatically deployed on every company device, updated automatically, and centrally managed by the IT department.
	Do you record information system events that may have an impact on information security management, do you monitor and secure them and if so, how?	The firewall controls and assesses system security events, monitors, and logs those events. The IT department gets a daily report on every event that happened.
	How do you ensure the security of your network?	The network is segmented, and all traffic is analyzed by a firewall. Antivirus, IPS/IDS, and Application Control features are active on the firewall.
	Do you use wireless networks? How are they secured?	We utilize different segmented wireless networks, some isolated to specific addresses and ports necessary for operation. The company laptop wireless network is secured with two-factor authentication and a ZTNA control from the firewall. All wireless networks are encrypted with the WPA2 standard.
	Please see our TOMs for further IT security measures	

Part 2 – DocumentsCorePack Online Service		
#	Question	Response
General information		
	Short Description of the Product	DocumentsCorePack is a professional document generation and processing tool for Microsoft Dynamics 365 & Power Platform.
	Description of the Service	The online service, configured on our homepage, is hosted on one of our Microsoft Azure Servers. This service is necessary for the connection to the customer's Dynamics 365 instance.
	Purposes of the Service	Once a customer sends a document generation request the service will grab the request from Dynamics 365, retrieve the data, generate the document and push it back to Dynamics 365. Afterwards, the document can be accessed by customers.
	Description of the Service Architecture (data flow diagram)	https://support.mscrm-addons.com/knowledgebase/documentscorepack-online-scheme-2/
	Service Configuration with Step-by-Step Video	https://www.mscrm-addons.com/Products/DocumentsCorePack/ServiceConfiguration
	Product and Azure-specific TOMS	https://www.mscrm-addons.com/Portals/0/Legal%20Documents/EN_TechnicalandOrganisationalMeasures(TOMsArt.32GDPR)ProductDeliveryviaMicrosoftAzure.pdf
Data Processing		
	Does DocumentsCorePack need to have access to process customers' data?	As outlined in the Online Scheme, temporary access to predefined data is required to generate the document.
	Does the processing involve categories of personal data?	The customer has full control over this aspect. Within the template designer, they determine which data to include in the generated document, which may include personal data.
	Is there any customer data being stored on your systems (data at rest)?	No. During standard document generation, customer data (e.g. information from Dynamics 365 used to generate documents) is only held in memory and not stored in any environment of mscrm-addons.com **Exceptions:** 1. Customer-enabled debugging Used for troubleshooting, can be manually deleted at any time on the service overview. 2. Large document package requests The Azure cache isn't big enough for specific concatenation types to complete the request without data retention.

		3. Customer-activated file storage in an Azure Blob managed by mscrm-addons.com In these cases, data is securely isolated per service and **automatically deleted after 7 days.** By default, documents are stored as annotations in the customer's Dynamics 365 system or, if enabled, in their own Azure Blob — mscrm-addons.com does not store any data in those cases.
	Will you transfer or process any personal data of the customer outside the EU?	This can be decided by the customer as well. During the service configuration, the customer selects the data center (location), in which the service should operate. By default, the data center with the best possible bandwidth connection to the customer's Dynamics 365 instance is pre-selected.
	Do you collect usage statistics?	Yes, we collect usage statistics (e.g. number of generated documents). These contain no document content or personal data and are used for internal analytics and to provide service insights (e.g. template usage) via the customer's service account.
Third Party		
	Does the service rely on any third parties?	Yes, the service runs on one of our servers, hosted in the Microsoft Azure Datacenter.
	Name of the third party?	Microsoft Ireland Operations Ltd
	Third party compliance	https://learn.microsoft.com/en-us/azure/compliance/
	Registered head office of the third party?	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland
	Countries where their services are delivered from?	Our Azure Servers are hosted in various data centers. Here is the whole list of data center locations we offer: https://support.mscrm-addons.com/knowledgebase/datacenter-locations/
	What level of access do they have to client data?	None, they are hosting the server but do not get direct access to customer data.
Security		
	What is the method used to transfer data from the source?	To communicate from the cloud service to Dynamics 365 we use Server2Server authentication or App-Access without the need to store login credentials on our end. The communication is secured via methods provided by the Dynamics 365 SDK (TLS 1.2, OAuth).
	Do you have monitoring and alerting in place for security events?	Yes. We have implemented a Security Information and Event Management (SIEM) solution with real-time alerting across our entire infrastructure, including all Azure servers running our services.
	How do you get licensing information from AAD?	For AAD based licensing, we are accessing the UserPrincipalName & Username field of the user record and the AssignedLicenses and ServicePlans.

		For performance reasons the final list of users & serviceplan assignments is saved as an encrypted value in customer's CRM, where the licensing overview is looking for a cache when being accessed. The information is therefore not stored in any other place than your CRM system!
	Is there a possibility to install the document generation service locally?	Yes, customers with security concerns are eligible to install DCP either on their own Azure VM or on local hardware. Please note that for performance reasons an installation on the VM is recommended.

Part 3 – AttachmentExtractor Online Service		
#	Question	Response
General information		
	Short Description of the Product	AttachmentExactor helps you to save expensive database space in your DataVerse by extracting attachments and email content from your environment to alternative databases while keeping the user experience unchanged.
	Description of the Service	The online service, configured on our homepage, is hosted on one of our Microsoft Azure Servers. This service is necessary for the connection to the customer's Dynamics 365 instance.
	Purposes of the Service	AttachmentExtractor will retrieve documents from the Dynamics 365 instance, move them to an alternative storage location and deliver them back to Dynamics 365 upon user request.
	Description of the Service Architecture (data flow diagram)	https://support.mscrm-addons.com/knowledgebase/attachmentextractor-online-scheme/
	Service Configuration with Step-by-Step Video	https://www.mscrm-addons.com/Solutions/AttachmentExtractor/Start-AttachmentExtractor-Trial
	Product and Azure specific TOMS	https://www.mscrm-addons.com/Portals/0/Legal%20Documents/EN_TechnicalandOrganisationalMeasures(TOMsArt.32GDPR)ProductDeliveryviaMicrosoftAzure.pdf
Data Processing		
	Does the processing involve categories of personal data?	That can be decided by the customer. The customer configures the service and therefore decides which data he would like to have extracted.
	During the extracting process, is there any customer data being stored?	No data is ever stored unless debugging is enabled. In that case, data will be auto-deleted after 7 days or immediately by clicking on "delete logs" on the service overview.
	Will you transfer or process any personal data of the customer outside the EU?	This can be decided by the customer as well. When creating the service, you can simply select the server (and therefore the location) on which the service should be installed. By default, the data center with the best possible bandwidth connection to the customer's Dynamics 365 instance is pre-selected.
	Do you collect usage statistics?	Yes, we collect usage statistics (e.g. extraction volume). These contain no document content or personal data and are used for internal analytics and to provide useful service insights via the customer's service account.
Third Party		

	Does the service have any dependency on any third parties?	Yes, the service runs in the Microsoft Azure Datacenter.
	Name of the third party?	Microsoft Ireland Operations Ltd
	Registered head office of the third party?	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland
	The country or countries that their services are delivered from	Our Azure Servers are hosted in different data centers. Here is the whole list of data center locations we offer: https://support.mscrm-addons.com/knowledgebase/datacenter-locations/
	The access that they have to client data	None, they are hosting the server but do not get access to customer data.
Security		
	What is the method used to transfer data from the source?	The cloud service is securely communicating with Dynamics 365 web services using methods provided by the Dynamics 365 SDK (TLS 1.2, OAuth authentication). We employ Server-to-Server authentication or App-Access for the communication thereby eliminating the need for login credentials storage
	Do you have monitoring and alerting in place for security events?	Yes. We have implemented a Security Information and Event Management (SIEM) solution with real-time alerting across our entire infrastructure, including all Azure servers running our services.
	How do you get licensing information from AAD?	For AAD based licensing, we are accessing the UserPrincipalName & Username field of the user record and the AssignedLicenses and ServicePlans. For performance reasons the final list of users & serviceplan assignments is saved as an encrypted value in the customer's CRM, where the licensing overview is looking for a cache when being accessed. The information is therefore not stored in any other place than your CRM system!
	Is there a possibility to install the document generation service locally?	Yes, customers with security concerns are eligible to install AE either on their own Azure VM or on local hardware. Please note that for performance reasons an installation in the VM is recommended.

Appendix 01

ISO27001:2022 – Policy Overview		
Number	Name	ISO27001 Reference
Our Policies are approved by our CEO Christian Ternek and will be reviewed at least yearly.		
POL-00	ISMS List of documents	C.6.1.1
POL-01	Scope of the ISMS	C.4.1; C.4.2; C.4.3; C.4.4; C.6.1.1
POL-02	Information Security Management System ("ISMS")	C.4.4; C.5.1; C.5.2; C.6.1.1; C.6.2; C.7.1; C.8.1; C.9.1; C.9.3; C.10.1; C.10.2; A.18.1.1; A.18.1.2; A.18.2.2
POL-03	Roles, Responsibilities, and Authorities	C.5.1; C.5.2; C.5.3; C.6.1.1; A.5.1.1; A.5.1.2; A.6.1.1; A.7.1.2; A.7.2.1
POL-04	Information Security & Acceptable Use	C.5.1; C.5.2; C.7.2; C.7.3; A.5.1.1; A.5.1.2; A.6.2.1; A.6.2.2; A.7.1.2; A.7.2.1; A.7.2.3; A.8.1.3; A.8.2.3; A.9.2.4; A.9.3.1; A.11.2.6; A.11.2.8; A.11.2.9; A.12.5.1; A.12.6.2; A.16.1.3
POL-05	Document Control	C.7.5.1; C.7.5.2; C.7.5.3; A.18.1.3;
POL-06	Information Security Communication Plan	C.7.3; C.7.4
POL-07	Internal Audits	C.9.2; A.18.2.1; A.18.2.2
POL-08	Cloud Security	C.5.2; A.5.1; A.5.7; A.5.23; A.7.4; A.8.11; A.8.12; A.8.16; A.8.23
POL-09	Risk Management Information Risk Register	C.5.2; C.6.1.1; C.6.1.2; C.6.1.3; C.8.1; C.8.3; A.5.1.1; A.5.1.2; A.6.1.1; A.6.1.5; A.7.2.1; A.14.1.1; A.18.2.1; A.18.2.2; A.18.2.3
POL-10	Physical Security	C.5.2; A.5.1.1; A.5.1.2; A.7.2.1; A.11.1.1; A.11.1.2; A.11.1.3; A.11.1.4; A.11.1.5; A.11.1.6; A.11.2.1; A.11.2.2; A.11.2.4; A.11.2.9
POL-11	Access Control	C.5.2; A.5.1.1; A.5.1.2; A.6.1.2; A.6.2.2; A.7.2.1; A.9.1.1; A.9.1.2; A.9.2.1; A.9.2.2; A.9.2.3; A.9.2.5; A.9.2.6; A.9.3.1; A.9.4.1; A.9.4.2; A.9.4.3; A.9.4.4; A.9.4.5
POL-12	Cryptography	C.5.2; A.5.1.1; A.5.1.2; A.7.2.1; A.10.1.1; A.10.1.2; A.13.2.1; A.13.2.2; A.13.2.3; A.14.1.2; A.14.1.3; A.18.1.5
POL-13	Asset Management	C.5.2; A.5.1.1; A.5.1.2; A.7.2.1; A.8.1.4; A.8.2.3; A.8.3.2; A.8.3.3; A.11.2.5; A.11.2.6; A.11.2.7; A.11.2.8;
POL-14	Data Management	C.5.2; A.5.1.1; A.5.1.2; A.7.2.1; A.8.2.1; A.8.2.2; A.8.2.3; A.8.3.1; A.8.3.2; A.8.3.3; A.11.2.7; A.11.2.8; A.13.2.4;
POL-15	Human Resource Security	C.5.2; C.7.1; C.7.2; C.7.3; C.9.1; A.5.1.1; A.5.1.2; A.7.1.1 A.7.1.2; A.7.2.1; A.7.2.2; A.7.2.3; A.7.3.1; A.8.1.4; A.13.2.4
POL-16	Business Continuity and Disaster Recovery	C.5.2; A.5.1.1; A.5.1.2; A.7.2.1; A.17.1.1; A.17.1.2; A.17.1.3; A.17.2.1;
POL-17	Incident Management	C.5.2; A.5.1.1; A.5.1.2; A.6.1.3; A.7.2.1; A.16.1.1; A.16.1.2; A.16.1.3; A.16.1.4; A.16.1.5; A.16.1.6; A.16.1.7

POL-18	Secure Development	C.5.2; A.5.1.1; A.5.1.2; A.7.2.1; A.14.2.1; A.14.2.2; A.14.2.3; A.14.2.4; A.14.2.5; A.14.2.6; A.14.2.8; A.14.2.9 A.14.3.1
POL-19	Operations Security	C.5.2; A.5.1.1; A.5.1.2; A.6.1.2; A.7.2.1; A.12.1.1; A.12.1.2; A.12.1.3; A.12.1.4; A.12.2.1; A.12.3.1; A.12.4.1 A.12.4.2; A.12.4.3; A.12.4.4; A.12.5.1; A.12.6.1; A.12.6.2 A.12.7.1; A.13.1.1; A.13.1.3; A.14.1.1; A.14.2.2; A.14.2.3 A.14.2.4; A.14.2.5; A.14.2.6; A.14.2.8; A.14.2.9; A.14.3.1 A.18.1.3
POL-20	Third Party Management	C.5.2; A.5.1.1; A.5.1.2; A.7.2.1; A.11.1.1; A.11.1.2; A.11.1.3; A.11.1.4; A.11.1.5; A.11.1.6; A.11.2.1; A.11.2.2 A.11.2.3; A.11.2.4; A.13.1.2; A.13.2.1; A.13.2.2; A.13.2.4 A.14.2.7; A.15.1.1; A.15.1.2; A.15.1.3; A.15.2.1