MARMIND®
master your marketing

CLOUD SECURITY

01.01.2019

www.marmind.com

CLOUD SECURITY & PRIVACY

Protecting personal and business data of users in MARMIND is a main concern for UPPER Network GmbH as a provider and operator of MARMIND cloud software. Therefore, UPPER Network chose Microsoft Azure Germany as the cloud platform for MARMIND that meets the highest security standards. UPPER Network takes all possible technical safeguards against unauthorized access to both personal data of users in MARMIND as well as all data stored and managed per account. The protection includes measures for preventing access, copying, changing, deleting, re-use, distribution, transmission, manipulation or disclosure of information by unauthorized third parties.

DATA SECURITY

How data access generally protected?

- MARMIND uses HTTPS encrypted access at all times
- Microsoft Azure Germany guarantees state-of-the-art security measures (firewalls, encryption, etc.) that prevents unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access, or disclosure of data
  See (https://www.microsoft.com/de-de/trustcenter/security/azure-security)
- To protect against online threats UPPER Network uses services from Microsoft Azure antimalware cloud services. Microsoft also uses attack detection, prevention of DDoS attacks (Denial of Service), regular penetration testing, data analysis and machine learning tools in order to support the prevention of threats to the Azure platform
- Microsoft Azure meets as part of their duty to protect customer data the world's first standard for data protection in the cloud: ISO / IEC 27001 and ISO / IEC 27018 https://www.microsoft.com/de-de/TrustCenter/Compliance/ISO-IEC-27018
- Data security is managed by Microsoft and UPPER IT staff is Microsoft certified

How is access to the backend systems protected?

- Access to the Microsoft Azure Germany cloud infrastructure is restricted to UPPER Network employees only (no third-party or external users have access)
- MARMIND itself has no administrator roles that allow access to the MARMIND backend systems (cloud infrastructure services, databases etc.)
- Access (login events) on the Azure infrastructure are monitored by monitoring and reports the number of hits can always be created
- For more information on access security to the Microsoft Azure Data Center can be found here: https://www.microsoft.com/de-de/trustcenter/cloudservices/azure and https://www.microsoft.com/de-de/cloud/deutsche-cloud

What methods or tools are used for system monitoring?

- Monitoring of the cloud infrastructure, servers and databases is performed by Azure monitoring on the management User Interface
- In addition, Nagios monitoring is used for detailed monitoring of server activity
- Further, an application-specific monitoring and logging for MARMIND cloud services was developed, to monitor access to the API interfaces, error handling, user activities, performance and other important system KPIs

© UPPER Network GmbH

- The MARMIND application automatically generates log files with important and relevant information for possible debugging (operations, events, exceptions, errors etc.)
- When examining incidents, the accuracy and the amount of logged data can be adapted to facilitate troubleshooting (only accessible and performed by UPPER IT staff)

Can the customer access log files?

- No, the log files are created and stored within the protected area of the Azure infrastructure
- Access to log files by unauthorized external persons is denied
- MARMIND also does not provide an optional administrator role that could be unlocked for temporary access to backend or monitoring data
- If necessary, log files can be generated and provided to the customer with approval by UPPER Network

Do our servers use public keys?

All MARMIND web servers managed by UPPER Network exclusively use SSL certificates that have been issued by Trusted Certification Authorities.

What methods to improve data security are in place?

- Microsoft conducts regular penetration tests to improve Azure security controls and processes. (https://www.microsoft.com/en-us/trustcenter/security/azuresecurity#defend_against_threats
- User or administrative access is always encrypted (http or VPN)
- Local firewalls are active on all Azure servers used for the operation of MARMIND
- Inactive sessions automatically expire after a period of time and are terminated
- More information on Azure security best practices: https://docs.microsoft.com/de-de/azure/security/

How is the security of the cloud infrastructure ensured in the future?

- Microsoft continuously improves the security standards of its cloud solution (https://www.microsoft.com/de-de/trustcenter/cloudservices/azure)
- Microsoft is constantly expanding the number of compliance certifications

© UPPER Network GmbH

SPEICHERUNG DER DATEN

Wo werden die Daten gespeichert?

- Die Speicherung der MARMIND Daten und Backups erfolgen auf mehreren, physisch voneinander getrennten, sicheren Microsoft Azure Standorten nur innerhalb Deutschlands (Backup-Daten werden verschlüsselt gespeichert)
- Live Daten sowie Backup-Daten (Nutzer- und Account-bezogenen Daten) der MARMIND Nutzer werden in Microsoft Azure Datacenter innerhalb Deutschlands gespeichert

Wie werden die Daten gespeichert und gesichert?

- Die Speicherung der Backup-Daten erfolgt mithilfe exklusiver Server Encryption Keys auf einer sicheren Azure Datacenter Infrastruktur
- Alle Daten-Backups werden verschlüsselt und in separaten Standorten abgelegt
- Die Data Security auf Azure Deutschland wird durch den Datentreuhänder (T-Systems) gemanagt und gewährleistet: https://www.microsoft.com/de-de/cloud/deutsche-cloud#close
- Weiterführende Informationen zur Azure Sicherheit: https://docs.microsoft.com/de-de/azure/security/

Wem gehören die Daten in der Cloud?

- Durch Microsoft Azure Deutschland wird garantiert, dass alle in der Cloud gespeicherten Daten von MARMIND ausschließlich unter Kontrolle von UPPER Network bleiben. Dies gilt für alle Daten, auch für Text-, Ton-, Video- oder Bilddateien sowie Software, die Microsoft von UPPER Network oder MARMIND Kunden im Rahmen der Nutzung von Azure erhält (https://www.microsoft.com/de-de/cloud/deutsche-cloud)
- Weder Microsoft, T-Systems noch UPPER Network verwendet Nutzer- bzw. Kundendaten, die in MARMIND eingegeben und verwaltet werden zu Werbezwecken oder zum Data Mining, noch werden zu diesem Zweck Informationen ohne die Zustimmung des Kunden daraus abgeleitet

ZUGRIFF AUF DATEN

Wer hat Zugriff auf die Daten in der Cloud?

- Auf die Personen- und Account-bezogenen Daten: Die jeweils autorisierten Nutzer des Kunden
- Auf die Backend-Systeme: Nur autorisierte UPPER Network IT-Mitarbeiter
- Der Zugriff auf Kundendaten durch Drittanbieter oder Partnerunternehmen ohne Zustimmung des Kunden ist ausgeschlossen
- Microsoft Techniker haben ohne ausdrückliche Genehmigung von UPPER Network keinen Zugriff auf MARMIND Nutzerdaten (https://www.microsoft.com/de-de/cloud/rechtssicherheit.aspx)
- Persönlichen Daten von Nutzern sind nur jenen UPPER Network Mitarbeitern zugänglich, die notwendigerweise Einsicht in diese Daten haben müssen, um ihre Tätigkeit ordnungsgemäß ausüben und die MARMIND Softwaredienste und -produkte bestmöglich anbieten zu können
- Für Nichtmitglieder der MARMIND Software sind die Nutzer Profildaten nicht erreichbar
- Auch wird die MARMIND Software nicht von externen Suchmaschinen durchsucht, wodurch Nutzer Profile auffindbar wären

© UPPER Network GmbH

© UPPER Network GmbH

Wie kann von Nutzern auf die Daten in MARMIND zugegriffen werden?

- MARMIND unterstützt die gängigen Web-Browser in der aktuellen Version (IE11+, Chrome, Firefox, Safari) für einen Zugriff per Desktop oder mobilen Endgeräten
- Die MARMIND Software nutzt dabei stets eine verschlüsselte Datenübertragung per HTTPS
- MARMIND bietet zusätzlich eine Mobile App der wichtigsten Funktionen für Google Android und Apple iOS Endgeräte
- Die Sicherheit und Kompatibilität mit Web-Browsern in der aktuellsten Version wird durch laufende Updates von MARMIND sichergestellt

Wie erfolgt die Authentifizierung von Nutzern?

- Der Zugriff auf MARMIND ist passwortgeschützt
- Für die Registrierung und Authentifizierung zu MARMIND ist die Vergabe einer E-Mail-Adresse und eines Passworts von min. 8 Zeichen erforderlich (keine automatische Passwort-Generierung)
- Die Authentifizierung von Benutzern erfolgt dabei per OAuth 2.0 Authentifizierung, die eine sichere API-Autorisierung für Desktop-, Web- und Mobile-Anwendungen erlaubt
- Je nach Benutzerrolle und den damit verbundenen Rechten kann der Zugriff auf die accountbezogenen Daten je MARMIND Account und pro Benutzer eingeschränkt werden
- Ein Cross-Domain Identity Management ist aktuell nicht verfügbar

Können andere Cloud Nutzer auf meine Daten zugreifen?

- MARMIND bietet keine Administrator-Rollen für Kunden, um auf übergeordnete (accountfremde) Daten von MARMIND zugreifen zu können
- MARMIND bietet autorisierten Nutzern jedoch die Möglichkeit, weitere Nutzer in den eigenen Account einzuladen und diesen Zugriff auf Kunden-bezogene Daten freizugeben
- Diese Zugriffsrechte können jedoch jederzeit wieder entzogen werden (Nutzer aus der eigenen Benutzerverwaltung entfernen)

Wie werden meine Daten von anderen Kundendaten getrennt?

- MARMIND verwaltet Nutzer- bzw. Kundendaten in Datenbanken und Services innerhalb der geschützten Cloud Infrastruktur von Microsoft Azure Deutschland
- Der unautorisierte Zugriff fremder MARNMIND Nutzern auf die eigenen Nutzer- bzw. Kundendaten ist durch ein mehrstufiges Security Konzept innerhalb der Applikation ausgeschlossen
- Der Zugriff auf Kundendaten muss Nutzern innerhalb von MARMIND dezidiert freigegeben werden. Beispiel: Für den Zugriff auf ein Dokument innerhalb eines Marketingprojekts in einem Firmenaccount muss ein neuer Benutzer:
    1. Registrierte Benutzer in MARMIND sein
    2. In den Firmen Account („Netzwerk“) eingeladen werden
    3. Für einen Projekt-Kontext („Team“) freigegeben werden und
    4. Für den Zugriff („Sichtbarkeit für“) auf das Dokument freigeschaltet werden
- Eine sichere Kommunikation wird durch die Verwendung von Industrie Standards (SSL) gewährleistet

© UPPER Network GmbH

Wie erfolgt die Zugriffsüberwachung auf die Daten?

- Ein Daten-Zugriffs-Management der Server, Datenbanken und Services von MARMIND erfolgt per System-Monitoring und Logging der Zugriffe
- Weitere Informationen zur Security finden Sie hier: https://docs.microsoft.com/de-de/azure/security/
- Weiterführende Informationen zum Threat Management finden Sie hier: https://www.microsoft.com/de-de/trustcenter/security/azure-security#defend_against_threats

Welche UPPER Network Mitarbeiter haben Zugriff auf die MARMIND Systeme?

- Physischen Zugang zu Azure Datencenter: Keiner
- Zugang zur Azure Backend: UPPER Network IT System Administratoren
- Zugang zu Azure Services: UPPER Network IT System Administratoren, UPPER Network MARMIND Support Team
- Zugang zu MARMIND: UPPER Network MARMIND Support Team

Was passiert nach Beendigung der Vertragslaufzeit mit den Daten?

- UPPER Network löscht die nutzer- bzw. kundenspezifischen Daten nach Beendigung der Vertragslaufzeit. Die Daten stehen einer weiteren Verwendung dann nicht mehr zur Verfügung
- Die Daten können vom Kunden zuvor selbständig gesichert oder bei Bedarf als Kopie angefordert werden
- Daten, die von Nutzern an Dritte weiterübermittelt wurden, bleiben bestehen, da diese zu dem Account eines Dritten gehören
- Microsoft hält sich strikt an internationale Standards und Prozeduren im Falle der Löschung von Daten unter Aufsicht, überschreibt Cloud Storage datensicher vor der Wiederverwendung und führt defekte Hardware mit Kundendaten einer Entsorgung (Zerstörung) unter Aufsicht und Einhaltung höchster Sicherheitsstandards zu (https://www.microsoft.com/de-de/TrustCenter/Privacy/data-management/default.aspx)
- Was passiert bei behördlichen oder gerichtlichen Anforderungen auf Datenzugriff?
- Bei Microsoft Cloud Deutschland kontrolliert ein designierter deutscher Datentreuhänder den Zugriff auf Kundendaten
- Wenn eine Regierung Kundendaten anfordert muss sie den geltenden Rechtsweg einhalten und Microsoft für Inhalte einen Gerichtsbeschluss oder für Kontoinformationen eine Vorladung vorlegen
- Falls Microsoft zur Offenlegung von Kundendaten verpflichtet ist, wird UPPER Network und der Kunde sofort darüber informiert und eine Kopie der Anforderung bereitgestellt, wenn dies nicht aufgrund von gesetzlichen Bestimmungen untersagt ist
- Microsoft legt Kundendaten niemals einer Regierung gegenüber offen, sofern dies nicht vom Kunden angewiesen wird oder vom Gesetz (es gilt deutsches Recht) erforderlich ist
- UPPER Network hält sich in diesem Fall ebenfalls an die gesetzlichen bzw. gerichtlichen Vorgaben
- Weitere Informationen hierzu finden Sie unter: https://www.microsoft.com/de-de/cloud/rechtssicherheit.aspx

© UPPER Network GmbH

DATENVERFÜGBARKEIT

Wie wird die Verfügbarkeit von Daten sichergestellt?

- Die Zugriffe sowie die Auslastung der Infrastruktur Services werden per System-Monitoring stetig auf mehreren Ebenen überwacht und protokolliert (Web Access, System Access, Azure Manage, Database Access)
- Durch die Bereitstellung der Daten über Microsoft Azure Deutschland wird eine größtmögliche Verfügbarkeit der Daten und Ausfallsicherheit der Systeme gewährleistet

Wodurch wird ein genereller Datenverlust verhindert?

- Azure verwendet hochverfügbares Storage
- Laufendes Backup der Daten
- Tägliches Backup der Datenbanken
- Laufende System-Backups

DATENAUSTAUSCH

Wie erfolgt ein Datenaustausch mit externen Systemen?

- Ein Datenaustausch mit angebundenen externen Systemen (z.B. MailChimp© E-Mail-Marketing Tool) erfolgt über eine RESTful API Schnittelle, über die auch Daten zum Web Browser Client bzw. Mobile Client ausgetauscht werden

Wie wird ein sicherer Datenaustausch sichergestellt?

- Jede Kommunikation, die von MARMIND genutzt wird erfolgt mit HTTPS Verschlüsselung

DATA SECURITY PLAN

Gibt es einen Data Security Plan?

- UPPER Network verfolgt einen kontinuierlichen Information Security Plan mit definierten Security Regeln und Prozeduren, um die Sicherheit der Daten und Systeme zu gewährleisten
- Die grundsätzliche Datensicherheit der Azure Cloud Deutschland Infrastruktur wird durch Microsoft gewährleistet: https://www.microsoft.com/de-de/cloud/deutsche-cloud
- Die IT-Mitarbeiter von UPPER Network sind Microsoft zertifiziert
- MARMIND wird durch UPPER Network laufend auf mögliche unautorisierte Angriffsszenarien getestet (z.B. Cross Site Scripting, etc.), die Security der Azure Plattform wird laufend von Microsoft geprüft und sichergestellt

Wie sieht der Software Entwicklungsprozess generell aus?

- MARMIND wird von UPPER Network stetig weiterentwickelt und laufend aktualisiert
- Die Entwicklung erfolgt nach agilen Software Entwicklungsmethoden nach SCRUM und Kanban inkl. kontinuierlicher Unit- und Integrationstest

© UPPER Network GmbH

- Das Software Development Lifecycle Management von UPPER Network sieht hierfür einen agilen Change Management Prozess inkl. Qualitätssicherung und mehrstufigen QA Phasen vor
- Erweiterungen werden auf Testsystemen vor dem Live-Release nach hohen QA-Standards getestet und müssen den Anforderungen des MARMIND Security Architektur Konzepts entsprechen
- Releases neuer Funktionen erfolgen nach SPRINT Iterationen inkl. Security und Qualitätsmanagement
- Eventuelle Major Bugs oder Blocker werden unabhängig von der Entwicklungsplanung sofort behandelt und gelöst (Separate Emergency Lane)
- Unit Tests und Integration Tests werden kontinuierlich durchgeführt und um periodische Tests ergänzt
- UPPER Network stellt damit sicher, dass Fehler minimiert und mögliche Security-Lücken durch Erweiterungen ausgeschlossen werden
- Notwenige Sicherheits-Updates der Systeme (Server, Datenbanken) und der Applikation (Services) werden von UPPER Network unmittelbar und unabhängig von der eigentlichen Weiterentwicklung der Software durchgeführt

Wie werden eventuelle Security Vorfälle entdeckt und dokumentiert?

- Zugriffe auf die Applikation sowie die Azure Infrastruktur und Services werden per Monitoring überwacht
- Unautorisierte Zugriffe werden auf verschiedene Ebene überwacht und dokumentiert (Web Access, System Access, Azure Manage, Database Access)
- Alle Kunden werden über Vorfälle sowie Störungen des Systems unmittelbar informiert

Was würde bei einem Security Vorfall geschehen?

- Der Zugriff auf die MARMIND bzw. Azure Cloud Deutschland Infrastruktur wird im Falle unbefugten Zugriffs unterbrochen
- Daten werden gesichert bzw. im Falle eines Datenverlustes aus Backup-Daten der letztgültige Stand der Daten wiederhergestellt
- Alle Kunden werden über Vorfälle sowie Störungen des Systems unmittelbar informiert

Erfolgen standardisierte Security Audits und Assessments?

- Da die komplette MARMIND Lösung auf der Microsoft Azure Cloud Deutschland Infrastruktur betrieben wird, erfolgen laufende Security Audits durch Microsoft und externe von Microsoft beauftragten Auditoren
- Eine Übersicht der von Azure erfüllten Compliance-Zertifizierungen sehen Sie auch unter: https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx https://www.microsoft.com/de-de/cloud/compliance-und-datenschutz.aspx

Ist es auch als Kunde möglich ein Security Audit zu initiieren?

- Ja, aber bitte beachten Sie, dass Tests dieser Art (z.B. Penetration Testing oder Scanning) auf die von uns genutzten Azure Systeme anzuwenden wären und dies vorab die Absprache und Autorisierung durch Microsoft voraussetzt

Was kann ich als Nutzer tun, wenn ich ein Sicherheits-Problem oder einen unbefugten Zugriff auf meine Daten vermute?

- Wenn Sie den Verdacht auf unbefugten Zugang zu Ihrem Account vermuten, wenden Sie sich bitte umgehend an support@marmind.com und schildern Sie uns den Fall
- Je besser dokumentiert Vorfälle an unsere Support Mitarbeiter gesendet werden, umso schneller und präziser können wir handeln und Fall bearbeiten und lösen
- Wenn Sie Informationen über die von Ihnen in MARMIND gespeicherten Daten haben möchten, wenden Sie sich bitte ebenfalls an unsere Support Mitarbeiter
- Sollten Sie Fragen bezüglich der Erhebung, Verarbeitung und Nutzung Ihrer personenbezogenen Daten durch die UPPER Network GmbH haben, sowie bei sonstigen Anfragen oder Hinweisen in Bezug auf die allgemeine Datenschutzerklärung, wenden Sie sich bitte ebenfalls an uns
- Die allgemeinen Datenschutzbestimmungen in aktueller Version finden Sie auf unsere Website unter: https://www.marmind.com/de/datenschutz/
- Die UPPER Network GmbH behält sich das Recht vor, diese Datenschutzbestimmungen jederzeit mit Wirkung für die Zukunft zu ändern

RECHTLICHE VERANTWORTUNG

Wer ist die verantwortliche Stelle im Sinne des Datenschutzgesetzes?

- Für die Sicherheit der auf MARMIND verwalteten Daten zeichnet die UPPER Network GmbH, Seering 5/4, 8141 Premstätten, Österreich verantwortlich
- Die UPPER Network GmbH als Anbieter und Betreiber der MARMIND Software unternimmt daher größtmögliche Anstrengungen um Kundendaten vor unbefugtem Zugriff, Verlust, Missbrauch, oder Zerstörung zu schützen
- UPPER Network übernimmt jedoch keine Verantwortung für die von Nutzern selbst Dritten zugänglich gemachte Informationen, sei es durch Einladung externer Personen als neue Nutzer in den eigenen Account oder das Teilen von Informationen mit externen Personen (z.B. Senden von Daten via E-Mail an Dritte, veröffentlichen von Dokumenten oder anderer Media Assets durch die „Teilen-Funktion“, etc.)

Sollten Sie Fragen oder Anregungen zum Datenschutz haben, können Sie sich gerne auch per E-Mail an support@marmind.com wenden.

MARMIND®
master your marketing

Eine Software Lösung der

UPPER Network GmbH
Seering 5/4
8141 Premstätten
Österreich

T +43 (0)1 804 88 333 50
F +43 (0)1 804 88 333 90
info@marmind.com

Geschäftsführer:
Mag. Peter Ramsenthaler

www.marmind.com