



# Regeln für Geschäftspartner / Lieferanten

Die Regeln für Geschäftspartner / Lieferanten sind auf der [Homepage der Manage Now GmbH](#) → [Impressum](#) neben weiteren Dokumenten wie AGBs und Einkaufsbedingungen in der jeweils aktuellen und gültigen Version zum Download verfügbar.

Jeder Geschäftspartner / Lieferant der Manage Now ist dafür selbst verantwortlich, sich regelmäßig zu versichern, daß ihm die jeweils aktuelle Version vorliegt, für die Leistungserbringung vollständig berücksichtigt wird und seine Mitarbeiter und Unterauftragnehmer deren Pflichten einhalten.

Jegliche Nachbesserungen, die aus der Nichtbeachtung der aktuellen Regelungen entstehen, gehen vollständig zu Lasten des Geschäftspartners / Lieferanten.

## 1. Grundsätzliche Regeln

- Alle Mitarbeiter müssen entsprechend sorgfältig und vertraulich mit Informationen und Systemen der Manage Now umgehen, soweit ihnen diese zur Verfügung gestellt werden oder ihnen ein entsprechender Zugriff eingeräumt wird.
- Eingesetzte Notebooks müssen mechanisch gegen Diebstahl geschützt werden (z.B. Kensington Lock).
- Es ist untersagt, sich Zugang zu Systemen, Applikationen oder Informationen zu verschaffen, die nicht zum vertraglich vereinbarten Service und / oder Zweck gehören.
- Informationen und Systeme der Manage Now dürfen ausschließlich zum vertraglich vereinbarten Zweck genutzt werden.
- Es ist untersagt, Informationen zu anderen als zu Vertragszwecken zu nutzen, zu speichern, zu bearbeiten, zu vervielfältigen, zu verbreiten.
- Es ist verboten, Informationen und / oder Systeme der Manage Now für private Zwecke zu verwenden.
- Eine automatische Weiterleitung von E-Mails an externe Mailadressen ist nicht erlaubt. Eine Weiterleitung im internen Verhältnis darf ausschließlich an Mitarbeiter erfolgen, die im gleichen Projekt / vereinbarten Vertragszweck mitarbeiten.
- Informationen müssen entsprechend ihrer Klassifizierung gehandhabt werden.
- Geltende und vereinbarte Datenschutzbestimmungen müssen eingehalten werden.
- Es muss sichergestellt sein, dass Telefongespräche oder Gespräche in öffentlichen Bereichen (öffentliche Verkehrsmittel, Flugzeug, Hotel etc.), die Manage Now Informationen oder Kundeninformationen betreffen, nicht von unberechtigten Dritten mitgehört werden können.
- Die von Manage Now zur Verfügung gestellten externen E-Mailadressen (Vorname.Nachname.external@manage-now.de) dürfen ausschließlich zur Registrierung in Manage Now-Applikationen, Manage Now Clouddiensten oder Manage Now Webseiten verwendet werden. Dies gilt identisch für die Hinterlegung dieser Adressen als Kontakt auf für Manage Now erstellte Webseiten oder Domainanmeldungen.

## 2. Mitnahme von Unterlagen

- Die Mitnahme von Daten und Dokumenten (Ausdrucke, Backups etc.) außerhalb von Manage Now Standorten bedarf der Genehmigung durch den Manage Now Ansprechpartner für das Projekt / den vertraglich vereinbarten Service und / oder Zweck.
- Wenn Daten oder Medien außerhalb von Manage Now Standorten mitgenommen werden, so muss sichergestellt sein, dass keine unberechtigten Personen / Dritte Zugang zu diesen Informationen erhalten.
- Um Diebstahl zu vermeiden, müssen Daten und tragbare Medien auf Dienstreisen entsprechend vor unberechtigtem Zugriff geschützt werden und dürfen nicht unbeaufsichtigt bleiben.



### 3. Import- / Exportkontrolle

Informationen der Manage Now können unter die Import- / Exportbestimmungen nach EU, US oder unter anderes nationales Recht fallen. Die betrifft auch Informationen, die über das Netzwerk übertragen werden. In jedem Fall sind die Import- / Exportbestimmungen vorab zu ermitteln und deren Einhaltung muss sichergestellt sein.

### 4. Manage Now Daten am Standort des Geschäftspartners

Es muss sichergestellt sein, dass unberechtigte Dritte, die sich an den Standorten des Geschäftspartners aufhalten, keinen Zugang zu Informationen oder Systemen der Manage Now erhalten.

- Nach Besprechungen mit Manage Now müssen alle Dokumente und Informationen (Flipcharts, Handouts etc.) aus Besprechungsräumen entfernt werden.
- Systeme der Geschäftspartner, die mit Systemen oder dem Netzwerk der Manage Now datentechnisch verbunden sind, müssen in angemessener Art und Weise vor dem Zugriff durch unbefugte Personen geschützt werden.
- Jeder Sicherheitsvorfall, Störung oder entdeckte Schwachstelle muss der Manage Now gemeldet werden.
- Wenn nicht anderweitig vereinbart, müssen nach Vertragsende alle Unterlagen und Daten in Absprache mit Manage Now entweder zurückgegeben oder entsprechend den Vorgaben sicher gelöscht / zerstört werden. Dies betrifft auch Daten in den Systemen der Geschäftspartner, soweit diese keiner gesetzlichen Aufbewahrungsfrist unterliegen.
- Der Geschäftspartner muss über einen Notfallplan zum Schutz produktiver Daten und Systeme verfügen, die in irgendeiner Art und Weise Einfluss auf Manage Now haben können.
- Server und Netzwerkkomponenten (Router, Bridges, Switches ...) müssen in einem zutrittsgesicherten Raum betrieben werden. Bei Bedarf oder vorhandenen Risiken müssen Vorkehrungen gegen störende Umwelteinflüsse (elektromagnetische, chemische oder klimatische Faktoren) implementiert werden.

### 5. Arten von Informationen und deren Klassifizierung

Informationen sind in verschiedenen Formen auf unterschiedlichen Medien gespeichert.

- Elektronisch auf Systemen oder als E-Mails,
- Festplatten,
- Smart Cards,
- magnetische Bänder,
- CDs/DVDs,
- Papierunterlagen,
- Zeichnungen,
- Kopien etc.

Unabhängig von der Form müssen diese Informationen entsprechend geschützt und klassifiziert werden. Hierfür stehen folgende Klassifizierungslevel zur Verfügung:

Englisch	Deutsch (transferiert)
Public	Öffentlich
Restricted	Allgemein/Intern
Confidential	Vertraulich
Secret	Geheim

### 6. Speicherung von Informationen

Dokumente und Daten müssen am Tätigkeitsort durch Aufbewahrung in verschlossenen Behältnissen vor unberechtigtem Zugang oder Diebstahl geschützt werden.



## 7. Vernichtung und Löschung von Informationen

- Nicht als PUBLIC klassifizierte Unterlagen in Papierform sind in Schreddern mit Partikelschnitt entsprechend der Klassifizierung zu entsorgen oder in verschlossenen Containern, die von zertifizierten Entsorgungsunternehmen bereitgestellt werden, zu sammeln und der vorgegebenen Vernichtung zuzuführen.
- Elektronische Medien müssen sicher gelöscht werden. Falls dies nicht möglich ist, müssen die Datenträger mechanisch vernichtet werden.
- Beschädigte Medien, die nicht gelöscht werden können, müssen mechanisch vernichtet werden.

## 8. Zugang zu Manage Now Systemen

- Zugangsdaten zu Manage Now Systemen sind personalisiert. Zugangsdaten dürfen nicht an Dritte weitergegeben werden.
- Sobald ein Zugang nicht mehr benötigt wird, müssen die Zugangsrechte unverzüglich entzogen werden.
- Passwörter müssen der Manage Now Passwortrichtlinie entsprechen und regelmäßig geändert werden.
- Bei Passwordeingabe muss darauf geachtet werden, dass kein unbefugter Dritter die Zugangsdaten mitlesen kann (z.B. in öffentlichen Bereichen).
- Passwörter müssen bei Verdacht auf Offenlegung sofort geändert werden.
- Passwörter dürfen grundsätzlich nicht automatisch gespeichert werden. Sollte die Speicherung von Passwörtern in Systemen notwendig sein, so muss das verschlüsselt erfolgen und darf für Dritte nicht zugänglich sein.
- Die Speicherung von Passwörtern für Manage Now Systeme darf ausschließlich in durch Manage Now bereitgestellten Password Management Tools erfolgen.

## 9. Sichere Handhabung von Medien

Grundsätzlich hat die Handhabung von Medien sich nach der Klassifizierung der gespeicherten Daten und Informationen zu richten. Siehe dazu Ziffer 5.!

- Speichermedien müssen vor Verlust, Beschädigung oder missbräuchlicher Verwendung außerhalb des vertraglich vereinbarten Zwecks geschützt werden.
- Auf Wechseldatenträgern, die zur Weitergabe von Informationen dienen, dürfen nur solche Informationen gespeichert sein, die für eine bestimmte Transaktion vorgesehen sind. Alle anderen Daten müssen vorab einer Weitergabe sicher entfernt werden.
- Datenträger müssen vor Weitergabe auf Schadsoftware gescannt werden.
- Datenträger, die verschickt werden sollen, müssen entsprechend verpackt und vor Verlust, Beschädigung und Zerstörung gesichert sein.
- Es muss sichergestellt sein, dass Manage Now Daten von allen Systemen, die anderweitig wiederverwendet werden sollen, sicher und vollständig entfernt werden.

## 10. Backup und Archivierung

- Daten, die während der Zusammenarbeit mit Manage Now erstellt werden, müssen in regelmäßigen Abständen gesichert werden. Jeder Nutzer ist für die Sicherung seiner lokalen Daten selbst verantwortlich.
- Wo immer möglich, sollten Daten auf Netzwerksystemen (Servern) gespeichert werden. Diese Systeme werden regelmäßig zentral gesichert.
- Externe Backupmedien müssen zugriffssicher aufbewahrt werden.
- Es muss sichergestellt sein, dass Langzeitbackups jederzeit lesbar sind. Entsprechend den Angaben der Hersteller müssen Daten regelmäßig auf neue Backupmedien kopiert werden. Entsprechende Hard- und Software zum Lesen der Daten muss vorhanden sein.

## 11. Netzwerkzugang

Geräte von Geschäftspartnern (z.B. Notebooks) dürfen nicht mit dem Netz der Manage Now verbunden werden.