

## SERVICE PAKETE FÜR DATENSICHERUNG

### Leistungsbeschreibung

Die nachfolgenden Service Pakete stellen die Grundlage für die Betreuung Ihrer Datensicherung durch die Weingarten PC-Service GmbH dar.

### Übersicht der Leistungen

	Basic	Standard	Premium
1. Tägliches Monitoring / Überwachung des Backups	✓	✓	✓
2. Dokumentation der Konfiguration der Datensicherung	–	jährlich & bei Änderungen	jährlich & bei Änderungen
3. Einspielen von Sicherheitsupdates und fehlerbereinigenden Patches der Backup-Software	–	✓	✓
4. Analyse und Koordination von Fehlerbehebungen	–	✓	✓
5. Kapazitätsanalyse und Zustandsanalyse der Backup-Medien	–	quartalsweise	quartalsweise
6. Manuelle Testrücksicherung eines ausgewählten Ordners	–	quartalsweise	quartalsweise
7. Durchführung einer Disaster-Recovery-Simulation eines Systems („Feuerwehübung“)	–	–	jährlich
8. Monatspauschale pro Gerät mit Datensicherung (zzgl. einmalige Einrichtung 49,90 €)	19,90 €	49,90 €	79,90 €
<b>Ziel des Pakets</b>	<b>Überblick behalten</b>	<b>Pflichtaufgaben erfüllen</b>	<b>Sicherheit gewinnen</b>

9. Option: Datensicherung ins Rechenzentrum	Server mit 500GB	Arbeitsplatz mit 100 GB
Monatspauschale	99,90 €	29,90 €
Weitere 100 GB Speicherplatz	14,90 €	14,90 €

10. Option: Datensicherung Office 365 Postfach	
Monatspauschale bis zu 100 GB	6,90 €

## Leistungsbeschreibung der Service Pakete für Ihre Datensicherung

Ziel ist die zuverlässige, sichere und kostengünstige Betreuung Ihrer Datensicherung. Unser Betreuungskonzept basiert auf bestimmten Voraussetzungen Ihrer IT-Struktur.

Es gilt für folgende Softwareprodukte:

- Acronis Backup & Recovery ab Version 11.5
- NetJapan Active Image Protector ab Version 2018

Diese Datensicherungs-Softwareprodukte müssen unter gültiger Softwarewartung (Subscription/Maintenance) stehen.

Sie, als Kunde, sind für das tägliche Anfertigen einer Datensicherung verantwortlich und zwar insbesondere mit mindestens drei in regelmäßigem Wechsel zum Einsatz gebrachten Datenträgern.

Im diesem Betreuungskonzept wird nur die Datensicherung des Betriebssystems sowie der betriebssystemnahen Applikationen Active Directory, DNS, DHCP abgedeckt. Sollten Sie die Sicherung von weiteren Softwareapplikationen wünschen, so benötigen wir vorab von Ihnen eine Auflistung der gewünschten Applikationen. Je nach Umfang behalten wir uns Anpassungen am Gebührenmodell vor und erstellen Ihnen gegebenenfalls ein Zusatzangebot.

Sollen durch dieses Betreuungspaket die Datensicherung von Applikationen wie Lexware, GDI, Datev oder weitere Software mitbetreut werden, so ist dafür zu sorgen, dass diese Softwareprodukte ebenfalls unter gültiger Softwarewartung (Subscription/Maintenance) stehen. Bitte senden Sie uns hierfür die Supportkontaktdaten/ Vertragsnummern zu.

Sofern Sie die Erstellung eines Notfallplans wünschen, wird dieser gerne gegen Berechnung erstellt. Zur Erstellung ist eine Auflistung des Kunden über die von ihm als Notfallplan-relevanten Daten/Applikationen erforderlich.

### 1. Tägliches Monitoring / Überwachung des Backups

Zu einem definierten Zeitpunkt lesen wir täglich den Sicherungsstatus aus. Dies erfolgt über die vom Softwarehersteller bereitgestellten Log-Dateien bzw. die Windows Ereignisprotokolle, welche auf Erfolg oder Misserfolg überprüft werden. Mögliche Zustände sind „Erfolgreich“, „Mit Ausnahmen abgeschlossen“ und „Fehlerhaft“. Für die auf Basis des Monitorings erkannten Probleme werden die jeweils notwendigen Maßnahmen von uns ergriffen, um kurzfristig eine Fehlerbehebung herbeizuführen. Sofern die Korrekturen dieser Funktionsmängel nicht Bestandteil des gebuchten Pakets sind, werden diese gemäß unserem aktuellen Stundensatz berechnet.

### 2. Dokumentation der Konfiguration Ihrer Datensicherung

Der Kunde hat uns bei Änderungen an dem Einsatzzweck, der Version oder der Nutzungskonfiguration zu informieren, so dass wir gegebenenfalls Anpassungen an der Datensicherung bzw. Überprüfung der Datensicherung vornehmen können.

Sie erhalten auf Wunsch eine aktuelle Dokumentation der Konfiguration Ihrer Datensicherung. Diese umfasst: Version der Datensicherungssoftware, Auflistung der Sicherungs-Jobs und der darin zu sichernden Daten, Sicherungsziele, konfigurierte Ausnahmen von der Datensicherung, Einstellung des Überschreibschutzes bzw. der Mediensätze und den Zeitplan der Datensicherung.

Übergeben wird das Ergebnis der Dokumentation als Papierdokument. Zum Zwecke des Einverständnisses wird das Dokument von beiden Parteien unterschrieben.

### 3. Einspielen von Sicherheitsupdates und fehlerbereinigenden Patches

Das Einspielen von Releases/Patches erfolgt bei laut Hersteller dringenden Sicherheitsaktualisierungen durch uns mit einer Frist von max. 12 Wochen nach Veröffentlichung und Bekanntgabe eines Patches durch den Hersteller. Ansonsten werden Patches nur nach unserem Ermessen installiert. Eine Haftung für eine fehlerfreie Installation der Updates kann nicht übernommen werden, da dies im Einflussbereich des jeweiligen Softwareherstellers liegt.

### 4. Analyse und Koordination von Fehlerbehebungen

Interpretation der Fehlermeldung und das Aufzeigen einer möglichen Fehlerbeseitigung durch unseren Techniker. Bei auftretenden Problemen an den zu sichernden Daten ist die Information und Koordination mit den für die Daten und Applikation zuständigen Firmen/Personen enthalten. Funktionsmängel in der für das Backup notwendigen Hard- und Software liegen im Verantwortungsbereich des jeweiligen Herstellers. Wir koordinieren Fehlerlösungen und informiert den Kunden.

### 5. Kapazitätsanalyse und Zustandsanalyse der Backup-Medien

Wir prüfen, ob die Speicherkapazität der Backup-Medien ausreicht, um den Sicherungsplan beizubehalten und geben im Falle von Platzknappheit eine Handlungsempfehlung.

### 6. Manuelle Testrücksicherung eines ausgewählten Ordners

Es erfolgt eine stichprobenartige Datenrücksicherung eines ausgewählten Ordners. Sie, als Kunde, können uns jederzeit mitteilen, welche Daten für die Stichprobe ausgewählt werden sollen – wir werden dies zum nächstmöglichen Rücksicherungszeitpunkt berücksichtigen. Teilt der Kunde dieses nicht mit, liegt die Entscheidung ohne Anspruch auf Zweckmäßigkeit und Vollständigkeit bei uns. Die Rücksicherung erfolgt auf einen zwischen uns und dem Kunden abzustimmenden Datenspeicherungs-Ort.

### 7. Durchführung einer Disaster-Recovery-Simulation eines Systems („Feuerwehrrübung“)

Die Disaster Recovery Simulation testet die Wiederherstellung eines vom Kunden zu bestimmenden Servers. Der Erfolg der stichprobenartigen Wiederherstellung wird auf Basis eines Client-Zugriffs auf die auf dem Server liegenden Daten/Applikationen festgestellt. Es kann Daten/Applikationen geben, für die mehr als ein Server wiederhergestellt werden muss, um eine sinnvolle Funktionalität aus Client-Sicht zu ermöglichen. In solch einem Fall werden wir ein gesondertes Angebot über den notwendigen Zusatzaufwand erstellen.

Grundsätzliche Voraussetzung für die Disaster-Recovery-Simulation ist eine vom Kunden zur Verfügung gestellte Ersatz-Hardware bzw. eine leere virtuelle Maschine, auf welche die Wiederherstellung vorgenommen wird. Diese muss zu den aktuell eingesetzten Komponenten gleichwertig sein. Für viele Einsatzzwecke kann auch von uns ein geeignetes Gerät gestellt werden.

### 8. Einmalige Einrichtungsgebühr und monatliche Betreuungs-Pauschale

Für die erstmalige Aufnahme Ihres Backup-Servers in unser Backup-Betreuungsmodell wird eine Einrichtungs-pauschale berechnet. Der Backup-Server wird mit einem entsprechenden Agenten für das Monitoring und die Fernwartung versehen und konfiguriert. Das Berichtswesen wird auf die vom Kunden gewünschte E-Mail-Adresse konfiguriert. Das Service-Paket „Datensicherung“ wird in unseren Systemen hinterlegt.

Die Monatspauschale gilt im jeweils gewählten Paketumfang je betreutem Gerät.

Weitere Dienstleistungen im Bereich Server, Clients, Drucker und lokaler Peripherie wie technische Hilfestellung, Fehleranalyse, Lösungserarbeitung, Umsetzung, Dokumentation erhalten Sie mit unseren „Service Paketen für Server und Clients“.

## 9. Option: Datensicherung ins Rechenzentrum

Dem Kunden wird ein Nutzungsrecht für eine Datensicherungssoftware zur Nutzung innerhalb dieses Konzepts bereitgestellt, die Hyper-V-Umgebungen, Windows Server, MS Exchange Server, MS SQL Server und MySQL Server sichern kann.

Es werden mindestens die letzten 28 Sicherungen sowie die jeweilige Sicherung des Monatsersten für die Dauer der Nutzung vorgehalten. Die Leistung umfasst die Sicherung unbegrenzter Anzahl von virtuellen Maschinen. Für die Sicherung von Datenbanken innerhalb von virtuellen Maschinen wird eine zusätzliche Sicherung als eigenes Datensicherungspaket empfohlen.

Wir stellen dem Kunden Festplattenkapazität in einem nach üblichem Standard gesicherten, ISO-27001 zertifizierten deutschen Rechenzentrum, derzeit Düsseldorf, bereit. Die Datenübertragung ins Rechenzentrum erfolgt mindestens 128-bit verschlüsselt. Die Datenspeicherung erfolgt mindestens 128-bit verschlüsselt mittels einem vom Kunden festgelegten und nur dem Kunden bekannten Verschlüsselungskennwort. Eine Wiederherstellung der Daten ohne Kenntnis des Verschlüsselungskennwortes ist nicht möglich. Ein Zurücksetzen des Kennwortes ist ebenfalls nicht möglich.

Das Backup erstellt verschlüsselte Kopien vom Kunden festgelegter Daten von Server- und PC-Systemen und sendet diese an das Rechenzentrum.

Funktionalitäten des Systems:

- a) Ein manuelles oder automatisches Backup von allen oder von ausgewählten Daten des Geräts auf die Backup-Plattform. Auf dem Client-PC/Server zwischenzeitlich geänderte oder gelöschte Dateien stehen auf der Backup-Plattform für 28 Tage zur Wiederherstellung zur Verfügung. Anzahl und Frequenz der vom Kunden auf der Backup-Plattform durchgeführten Backup/Restore-Vorgänge sind dabei unbeschränkt.
- b) Die Übermittlung der zu sichernden Daten (Backup-Daten) erfolgt unter Verwendung von Datenreduktions- und Datenkompressions-Technologien, die dem Stand der Technik entsprechen. Hierbei werden die seit der letzten Datensicherung veränderten Datenblöcke ermittelt und ausschließlich diese für den aktuellen Sicherungsvorgang übertragen. Die für das erste Vollbackup erforderliche Dauer ist abhängig vom Datenvolumen sowie der Schnelligkeit des jeweiligen Internetzugangs. Das Vollbackup kann wahlweise auch durch einen unserer Techniker gemäß der aktuellen Stundensätze vorgenommen werden.
- c) Die vom Kunden übermittelten Daten werden so gespeichert, wie sie vom Kunden zur Verfügung gestellt werden. Eine Überprüfung der Daten auf eine evtl. Virenverseuchung oder ähnliches erfolgt nicht.
- d) Die Speicherung der Backup-Daten des Kunden auf der Backup-Plattform erfolgt in komprimierter und verschlüsselter Form. Ein Verschlüsselungs-Code verhindert den Zugriff von Unberechtigten auf die vom Kunden abgespeicherten Daten. Bei Verlust des Verschlüsselungs-Codes können die Daten nicht mehr wiederhergestellt werden, auch nicht durch uns.
- e) Der Zugang zur Backup-Plattform erfolgt über das Internet. Die für den Zugang erforderlichen Anschlüsse sowie die für die Nutzung von Backup erforderlichen Verbindungen sind nicht Gegenstand dieses Vertrages. Voraussetzung für jeden Zugang zur Backup-Plattform ist die Authentifizierung des Kunden bzw. der von ihm autorisierten Nutzer mittels eines Passwortes.

Für das Rechenzentrum wird eine 99-prozentige Verfügbarkeit im Jahresmittel abzüglich der Wartungszeit vertraglich vereinbart. Wir sind berechtigt, nach vorheriger Ankündigung Wartungsarbeiten durchzuführen. Während der Wartungsarbeiten stehen die Rechenzentrumsleistungen nicht zur Verfügung. Störungsmeldungen nehmen wir während der üblichen Betriebszeiten entgegen und versichern eine schnellstmögliche Beseitigung im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten.

Im Paket enthalten ist ein Datenvolumen (bei Servern aktuell 500 GB, bei Arbeitsplätzen aktuell 100 GB) für die ausgewählte Datenmenge. Die über das Inklusiv-Volumen hinausgehende Datenmenge, wird je angefangene 100 GB zusätzlich abgerechnet.

Wir empfehlen die Verwendung eines Netzwerkspeichers (NAS) für die Datensicherung am Standort des Kunden. Das Gerät sollte in einem von den zu sichernden Geräten/Daten getrennten Brandabschnitt aufgestellt werden. Sollte der Netzwerkspeicher nicht in einem getrennten Brandabschnitt aufgestellt werden, ist der Kunde für alle dadurch entstehenden Haftungsrisiken verantwortlich.

## 10. Option: Datensicherung Office 365 Postfach

Sicherung eines Postfachs mit bis zu 100 GB Speichervolumen.