Leistungsbeschreibung „dvo Rechenzentrum allgemein”

I Allgemeines, Betrieb und Störungsbeseitigung

1 Vorbemerkung:
Falls bei einzelnen Services Leistungen von Dritten genutzt werden sollten, so sichert der Auftragnehmer zu, dass diese Services in der Republik Österreich bzw. bei gesondertem Hinweis innerhalb der EU gehostet sind und dem österreichischen Datenschutzgesetz bzw. der europäischen Datenschutzgrundverordnung unterliegen.

2 Web-Zugriff auf Service-Status:
Über ein Online-Ticketing-System kann der Kunde auf Wunsch Zugriff auf eine Übersicht aktueller und vergangener Servicefälle nehmen. Gleichzeitig ist ein Melden von neuen Problemen oder Aufgaben über dieses System möglich. Auf neu gemeldete Probleme oder Aufgaben wird die Interventionszeit nach Kapitel I Punkt 8 angewendet.
Allgemeine Wartungstätigkeiten, die außerhalb des allgemeinen Verfügbarkeitszeitraumes (Mo-Do 8-17 Uhr und Fr 8-14 Uhr) planmäßig stattfinden, werden per E-Mail an die hinterlegte Hauptkontakt-E-Mail-Adresse des Kunden spätestens zwei Tage im Vorhinein informativ angekündigt.

3 Fernwartungssoftware, Taskleistenapplikation:
Die Fernwartungssoftware ermöglicht die zeitnahe Problemlösung durch Techniker des Auftragnehmers aus der Ferne über eine nach dem üblichen Standard gesicherte Internetverbindung. Der Auftragnehmer versichert, diesen Zugang mit hoher Sorgfalt zu verwalten und versichert außerdem, sämtliche in Kontakt mit den Systemen des Kunden kommenden Mitarbeiter im Hinblick auf die Einhaltung des österreichischen Datenschutzgesetzes sowie zur Verschwiegenheit zu verpflichten.
Die benötigten Lizenzen zur Nutzung der Fernwartungssoftware sind im jeweiligen Produkt enthalten. Der Auftragnehmer stellt entweder eine über das IT-Management-System zugängliche Fernwartungs-Funktion für administrative Zwecke bereit, oder stellt eine herunterladbare Client-Software für die Ausführung auf nicht verwalteten Geräten zur Verfügung.
Auch bei Services, die vorwiegend im dvo Rechenzentrum laufen, kann im Supportfall ein Zugriff auf das lokale Anzeigegerät nützlich oder notwendig sein.
Bezüglich der Art des Fernwartungs-Zugriffs vereinbaren Kunde und Auftragnehmer ggf. eine Handhabung gemäß dem Dokument „Fernwartungsvereinbarung“.

4 Softwarelizenz-Ausstellung und Verwaltung für gehostete Services in den dvo Rechenzentren:
Die ordnungsgemäße Software-Lizenzierung der zur Bereitstellung der Services aus dem Rechenzentrum erforderlichen Drittanbieter-Software für die Betriebsumgebung (Service-Plattform) obliegt dem Auftragnehmer und befindet sich in dessen Verantwortung.
Bei einzelnen Services werden dem Auftraggeber jedoch Softwareprodukte in der gehosteten Umgebung zur Verfügung gestellt, die auf Namen und Rechnung des Auftraggebers lauten und sich in dessen Besitz befinden. Solche Softwareprodukte werden in Absprache mit dem Auftraggeber betrieben, die Verantwortung für die ordnungsgemäße Lizenzierung auch im Hinblick auf das Gewähren eines Outsourcing-Betriebs liegt zur Gänze beim Auftraggeber.

5 Monitoring:
Überwachung der Rechenzentrums-Services rund um die Uhr in einem 5-Minuten-Takt hinsichtlich der Lauffähigkeit der Windows-Dienste, Aktualität der Anti-Virus-Signaturen (1x täglich), Physischer Festplattenzustand (SMART, 1x täglich), Überprüfung der Erreichbarkeit einer Internet-Webseite, Überprüfung der Servertemperatur und CPU-Lüfterdrehzahl, Leistungsüberwachung der Server hinsichtlich Prozessorauslastung, Speichernutzung, Festplattenleistung und Netzwerkkarten-Auslastung.
Für etwaige Probleme, die mit dem Monitoring erkannt werden, wird die Interventionszeit nach Kapitel I Punkt 8 automatisch angewandt.
Fehlermeldungen werden von technischen Mitarbeitern des Auftragnehmers interpretiert.
Das Monitoring wird für relevante Systeme der Rechenzentrums-Bereitstellung automatisch durchgeführt und gehört zum Standard-Leistungsumfang.

6 Automatische Tasks, Bereinigungen von temporären Dateien und Eventlogeinträgen:
Eine regelmäßige Bereinigung von temporären Dateien, des Browser-Cache (Flash, Java, Dateien) und Eventlogeinträgen inklusive Protokollierung über den Erfolg der Maßnahme im IT-Management-System des Auftragnehmers wird für relevante Systeme der Rechenzentrums-Bereitstellung automatisch durchgeführt und gehört zum Standard-Leistungsumfang.

7 Alarmierung dvo IT:
Eine Alarmierung erfolgt aus dem IT-Management-System per E-Mail standardmäßig an die entsprechende Serviceabteilung des Auftragnehmers. Es erfolgt die Weiterverarbeitung der Fehler direkt im Ticket-System des Auftragnehmers. Danach erfolgt die Bearbeitung des eingegangen Fehlers, wobei die Interventionszeit nach Kapitel I Punkt 8 automatisch angewendet wird. Ggf. erfolgt eine Abrechnung nach Kapitel I Punkt 10, sofern ein spezifisches Software- oder Anwenderproblem vorliegt, das nicht mit der Bereitstellung der Services in Zusammenhang steht.
Die Alarmierung wird für relevante Systeme der Rechenzentrums-Bereitstellung automatisch durchgeführt und gehört mit Ausnahme von individuellen Software- oder Anwenderproblemen zum Standard-Leistungsumfang.

8 Interventionszeit bei kritischen Problemen:
Als kritisch wird ein Problem vom Auftragnehmer eingestuft, wenn dadurch ein Arbeitsausfall für mehr als zehn Personen verursacht wird oder wichtige Kernprozesse des Betriebs erheblich beeinträchtigt sind.
Bei kritischen Problemen muss seitens des Auftragnehmers innerhalb von vier Stunden während des Servicezeitraums Mo-Do 8-17 Uhr und Fr 8-14 Uhr mit der Problemlösung entweder direkt im Rechenzentrum (eigenständig), per telefonischer Hilfestellung oder per Fernwartung begonnen werden.
Die Interventionszeit beginnt mit Mitteilung an den Auftragnehmer per E-Mail (support@dvo.at bzw. technik@dvo.at), Telefon (Tel.-Nr.: +43 1 544 69 79 - 510) oder über das Online-Ticketing-System und läuft während des vereinbarten Servicezeitraums.

Möchte der Kunde ungeachtet der vorstehenden Regelungen im Einzelfall eine kritische Einstufung des vorliegenden Problems nach eigenem Ermessen durchführen, so wird dieser Fall mit einem Aufschlag von 20% auf den unter Kapitel I Punkt 10 genannten Servicepreis verrechnet. Bei enthaltenen Dienstleistungen im Rahmen der Servicebereitstellung der Rechenzentrums-Services wird bei manuell als kritisch eingestuften Problemmeldungen ein Dringlichkeitszuschlag von pauschal netto 50 EUR abgerechnet.

Bei unkritischen Problemen muss innerhalb von 48 Stunden während des Servicezeitraums Mo-Do 8-17 Uhr und Fr 8-14 Uhr mit der Problemlösung oder Terminierung der Problemlösung begonnen werden.

9 Störungsbeseitigung und ITIL-Standards:
Die Maßnahmen zur angestrebten Störungsbeseitigung (ITIL-Klasse „Incident“) sind als Standard-Leistung in allen Services des dvo Rechenzentrums pauschal enthalten und werden nicht nach Kapitel I Punkt 10 abgerechnet.
Der Auftragnehmer behält sich vor, bei übermäßiger individueller Nutzung von „Incident“-Meldungen um ein Gespräch zu bitten, um den Sachverhalt auf allgemeiner Basis zu klären und ggf. eine Anpassung der bezogenen Services vorzuschlagen.
Die Leistungen werden in der Zeit von Mo-Do 8-17 Uhr und Fr 8-14 Uhr erbracht. Es gilt die Interventionszeit nach Kapitel I Punkt 8.
System-, Software- oder Konfigurationsänderungen an technisch relevanten Einrichtungen im oder für das dvo Rechenzentrum dürfen nur durch den Auftragnehmer durchgeführt werden. Dies bedeutet, dass eventuelle Administrationskennwörter nur beim Auftragnehmer für Systemzugriffe vorhanden sind.
Aus Sicherheitsgründen werden Systemzugangskennungen zu Rechenzentrums-Services jeglicher Art keinesfalls an Auftraggeber oder Dritte ausgehändigt.

Die – in allen Services enthaltene – Leistung für Störungsbeseitigungen und Administrationstätigkeiten bezieht sich auf technische Dienstleistungen, die an der Rechenzentrumsinfrastruktur sowie an weiteren Anwendungen & Diensten laut Anlage 1 durchgeführt werden. Weitergehende Tätigkeiten an Softwareprogrammen oder angeschlossenen bzw. verbundenen Geräten wie NAS, SAN-Systeme sind nicht durch den Standard-Leistungsumfang der Rechenzentrums-Services abgedeckt.
Änderungen des konfigurierten Standards (ITIL Klasse „Service-Request“ und „Change Request“) sind grundsätzlich nicht im Standard-Leistungsumfang der Rechenzentrums-Services enthalten und werden gesondert angeboten bzw. abgerechnet.
Der Auftragnehmer wird nach üblichen Standards die Problemlösungen an den Softwareprogrammen durchführen. Eine Haftung für einen fehlerfreien Betrieb kann nicht übernommen werden, da dies nicht im Einflussbereich des Auftragnehmers, sondern in dem der jeweiligen Softwarehersteller liegt.

Differenzierung der Service-Klassen an Beispielen:
Incident: bspw. Kunde meldet, er kann keine Mails mehr versenden
Service-Request: Kunde stellt einen neuen Mitarbeiter an und dieser muss angelegt und eingerichtet werden
Change-Request: es soll auf Kundenwunsch eine neue, bisher nicht genutzte Software in Betrieb genommen werden

10 Stundensatz für weitere Leistungen:
Der Stundensatz für die Erbringung von – nicht in den jeweils gebuchten Rechenzentrums-Services enthaltene - Dienstleistungen im Bereich Server, Netzwerktechnik und Telekommunikation wie technische Hilfestellung, Fehleranalyse, Lösungserarbeitung, Umsetzung und Dokumentation beträgt in der Zeit von Mo-Do 8-17 Uhr und Fr 8-14 Uhr zur Zeit 120 EUR/h. Abgerechnet wird nach den ersten 30 Minuten im 15 Minuten-Takt.
Etwaige Fahrtkosten werden mit EUR 0,42 pro Entfernungskilometer berechnet. Die Fahrzeit wird mit dem halben vorgenannten Stundensatz abgerechnet.
Ein Fernzugriff auf die Kundensysteme erspart dem Kunden die Fahrtkosten, die Zeit wird wie zuvor genannt abgerechnet.
Außerhalb des Zeitraums wird ein erhöhter Stundensatz von EUR 150,00 (Mo-Do zwischen 17-8 Uhr und Fr 14-24 Uhr) bzw. 100% Zuschlag zum Standard-Stundensatz (Samstag, Sonntag und Feiertag) berechnet.
Neben der oben genannten Klasse „Standard-Leistungen“ wird für Dienstleistungen im Bereich Consulting, Konzeption und Umsetzung komplexer technischer Lösungen wie Hybrid-Rechenzentrumsleistungen, SAN-Lösungen, Virtualisierungsprojekte ein Stundensatz von 150 EUR/h mit 30% Zuschlag für Einsätze außerhalb der Geschäftszeiten (wochentags) und 100% Zuschlag für Wochenend- und Feiertagseinsätze abgerechnet.

11 Allgemeiner Hinweis auf „Funktionsgarantie“ und „Problemlösungszeit“ von lokal eingesetzter Hard- und Software in Zusammenhang mit der Nutzung von Rechenzentrums-Services

Für jegliche lokal eingesetzte Hard- oder Softwarekomponente, unabhängig davon, ob sie sich bereits vor der Inanspruchnahme von Rechenzentrums-Services im Besitz und Einsatz des Auftraggebers befand, ob die Hard- oder Softwarekomponente auf Empfehlung des Auftragnehmers durch den Auftraggeber angeschafft und eingesetzt wurde, oder ob der Auftragnehmer eine Hard- oder Softwarekomponente an den Auftraggeber gegen ein monatliches Entgelt vermietet hat, kann vom Auftragnehmer keinerlei Haftung oder Funktionsgarantie übernommen werden.

Es handelt sich ausschließlich um Produkte Dritter, die auch ihrerseits keinerlei Funktionsgarantie übernehmen können, da Fehler oder Funktionsversagen im komplexen Zusammenspiel der Komponenten niemals ausgeschlossen werden können.

In diesem Zusammenhang wird der Auftragnehmer nur bei individueller Beauftragung im Fehlerfall im Rahmen der Interventionszeit nach Kapitel I Punkt 8 reagieren und ggf. unter Einbeziehung des Hersteller-Supports mit der Problemlösung nach angemessenen Standardverfahren beginnen.

Eine maximale Zeit bis zur Problemlösung kann vom Auftragnehmer weder genannt noch in irgendeiner Form garantiert werden, ggf. ist die Zeit bis zur Problemlösung auch maßgeblich von der Reaktions- und Analysezeit des Herstellersupports abhängig, welcher ebenso keinerlei Garantien im Hinblick auf einen Zeitraum bis zur Problemlösung gewähren kann.

Es ist jedoch im Einzelfall möglich, nach entsprechenden Analyseprozessen eine Einschätzung zur Lage des Problems abzugeben und – falls möglich - ein Aviso des Lösungszeitpunkts zu nennen. Es ist dann in Absprache mit dem Auftraggeber – je nach Schwere bzw. Beeinträchtigungsgrad des Problems – möglich, alternative Aktionen zur Wiederherstellung eines (ggf. auch temporären) funktionalen Zustands einzuleiten, die eventuell einen genauer einschätzbaren Lösungszeitpunkt des Problems zulassen, als dies im konventionellen Lösungsprozess der Fall ist. Der konventionelle Lösungsprozess kann nach Absprache mit dem Auftraggeber in einem solchen Fall parallel fortgesetzt werden.

12 Gültigkeit Servicebedingungen

Nachrangig zu den Regelungen dieser Leistungsbeschreibung gelten die Servicebedingungen der AGB in der jeweils aktuellen Version. Außerdem gelten nachrangig für die eingesetzten Softwareprodukte die Lizenz- und Nutzungsbedingungen der jeweiligen Hersteller. Die allgemeinen Geschäftsbedingungen sind jederzeit abrufbar unter www.dvo.at/agb.

II E-Mail Verarbeitungslösung dvo Managed Mail und dvo Managed Mail Hosted Exchange

1 Allgemein

dvo Managed Mail und dvo Managed Mail Hosted Exchange sind E-Mail-Management-Lösungen, die vollständig innerhalb des dvo Rechenzentrum betrieben werden, um die Sicherheit und Verfügbarkeit des E-Mail-Verkehrs besser schützen und nachvollziehen zu können sowie einen vollständig österreichischen E-Mail-Dienst zu garantieren.

Es stehen zwei Produkte zur Verfügung:

- dvo Managed Mail: Ausfallsichere E-Mail Filter-, Sicherheits- und Verwaltungslösung mit Erfordernis eines eigenen lokalen Mailservers. (siehe Punkt 2 und 3)
- dvo Managed Mail Hosted Exchange: Kombiniert obiges Produkt mit einem vollwertigen Hosted Exchange Server – ein lokaler Mailserver ist nicht mehr erforderlich. (siehe Punkt 4)

Das Produkt „dvo Managed Mail Hosted Exchange" gehört zum Standard-Leistungsumfang einiger Produkte des dvo Rechenzentrums, ist aber auch völlig unabhängig von anderen Produkten des dvo Rechenzentrums bezugsfähig.

2 Hosted Mailmanagement „dvo Managed Mail" mit E-Mail-Ausfallschutz

Es handelt sich um eine rechenzentrumsbasierte Spam-, Malware- und Sicherheits-Filterung eingehender E-Mails. Die hochwertige Malware- und Sicherheitsfilterung beinhaltet einen Sandboxing-Test, in dem unbekannte Dateianhänge vor der Weiterleitung in einer externen virtuellen Umgebung (garantiert innerhalb der EU / Deutschland) ausgeführt und getestet werden, bevor sie dem Empfänger zugestellt werden.
Die Klassifizierung als Spam-Mail findet über ein adaptives, punktebasiertes Bewertungssystem statt. Pro Benutzer sind konfigurierbare, tägliche Berichte per E-Mail über die Anzahl der gefilterten Mails verfügbar, auf deren Details und Konfiguration über einen individuellen Login pro Benutzer zugegriffen werden kann.
Individuelle Filtereinstellungen (Schutzstärke) und individuelle Black- und Whitelists pro User sind möglich. Ein vom Auftraggeber zu ernennender Technik-Admin kann zusätzlich Einstellungen auf user-übergreifender Basis vornehmen sowie globale Black- und Whitelists anlegen.

3 E-Mail-Ausfallschutz über „dvo Managed Mail"

Die E-Mail-Ausfallschutz-Funktion stellt die Aufbewahrungsfunktion von eingehenden E-Mails dar, falls der Kunden-Mailserver ausfällt bzw. nicht per Internet für die reguläre Zustellung von E-Mails erreichbar ist.
In diesem Fall werden sämtliche eingehenden E-Mails an den Kunden zwischengespeichert bzw. aufbewahrt, bis der Kundenmailserver wieder erreichbar ist. Es erfolgt dazu eine automatische periodische Prüfung.
Sobald der Kundenmailserver wieder erreichbar ist, werden die zwischengespeicherten eingegangen E-Mails an den Kundenmailserver zugestellt. Die E-Mails werden für einen Zeitraum von standardmäßig 3 Tagen zwischengespeichert. Eine etwaige Verlängerung dieses Zeitraums ist nach Absprache möglich.

4 "dvo Managed Mail Hosted Exchange"

Bereitstellung eines Hosted Exchange Postfaches mit inkludierten Zusatzdiensten aus Punkt 2 und 3 aus dem dvo Rechenzentrum. Gemeinsames Adressbuch (interne und externe Kontakte), Verteilerlisten. Zugriff per Outlook Web Access (SSL-verschlüsselt), Outlook-MAPI-Zugriff, POP3, SMTP und IMAP Zugriff (Zugriff nur verschlüsselt möglich). Push-Funktion ActiveSync für mobile Endgeräte auf E-Mails, Kalender, Kontakte und Aufgaben - Voraussetzung ist, dass das mobile Gerät die ActiveSync Funktion unterstützt. Speicherplatz: 2 GB. E-Mails können mit einem Datenvolumen von maximal 20 MB pro E-Mail inklusive der Anhänge versendet werden. Es können maximal 10 E-Mails pro Minute pro Postfach versendet werden. Die Anzahl der Empfänger ist auf 100 pro Mail und insgesamt auf 1500 pro Tag pro Postfach begrenzt. Spamversand ist verboten.

Bei Anbindung eines mobilen Endgeräts (Android, IOS, Windows Mobile) wird aus Sicherheitsgründen vom Gerät ein PIN-Code oder Passcode zur Benutzerauthentifizierung angefordert (falls ein solcher nicht bereits vergeben ist) und der Zeitraum bis zur Gerätesperre und Anforderung dieses Codes auf eine Minute beschränkt.

III Datensicherung

1 Datensicherungskonzept und -Strategie im dvo Rechenzentrum

Das Datensicherungskonzept des dvo Rechenzentrums besteht aus drei voneinander unabhängigen Teilen:

- Datensicherung: konventionelle Datensicherung von Dateien, E-Mails, Datenbanken, etc. mittels verschlüsselter Backup-Software an den jeweils anderen dvo Rechenzentrums-Standort.
  Für diesen Teil des Datensicherungskonzepts gilt die unten genannte Archiv-Richtlinie.
- Abbildsicherung: Sicherung jeder Serverinstanz des dvo Rechenzentrums zur raschen Wiederherstellbarkeit ganzer Systeme. Dieser Sicherungstyp wird wöchentlich ausgeführt.
- Replikation: Hierbei werden sämtliche relevante System- und Betriebsdaten laufend an den jeweils anderen dvo Rechenzentrums-Standort in einer Form übertragen, welche die Inbetriebnahme sämtlicher relevanter Systeme am anderen als dem ursprünglichen Rechenzentrumsstandort erlaubt. Die Übertragung und Speicherung erfolgt ausschließlich verschlüsselt und findet durchgängig bzw. kontinuierlich statt.
  Dieser Sicherungstyp erlaubt den längerfristigen Totalausfall eines Rechenzentrums-Standortes (Site-Recovery) und stellt eine Disaster-Recovery-Notfallmaßnahme dar.

2 Archivrichtlinie für Datensicherung im dvo Rechenzentrum

Die konventionelle Datensicherung im dvo Rechenzentrum wird, wie oben bereits angeführt, auf Basis einer einheitlich angewandten Archivrichtlinie durchgeführt. Diese Archivrichtlinie erlaubt die Wiederherstellung alter Stände wie folgt:

- Sicherung Mo-Fr ab 22:00 Uhr: Zwei Wochen rückreichend = 10 Stände max.
- Sicherung jeder Freitag ab 22:00 Uhr: Ein Quartal rückreichend = 13 Stände max.
- Sicherung jeder letzte Freitag im Monat ab 22:00 Uhr: Ein Jahr rückreichend = 12 Stände max.
- Sicherung jeder letzte Freitag im Jahr ab 22:00 Uhr: Fünf Jahre rückreichend = 5 Stände max.

Die angeführten Stände verstehen sich als kumulativ wirksam und erlauben eine hohe Bandbreite an Wiederherstellungsmöglichkeiten alter, gelöschter oder überschriebener Daten bei degressiver Ständeintensität analog zur Wahrscheinlichkeit der Nutzung alter Stände.

3 Datensicherung und Abbildsicherung

Wie bereits oben beschrieben, wird zusätzlich zur konventionellen Datensicherung auf Datei-, Datenbank- bzw. Maillevelebene eine Abbildsicherung (Imagebackup) jeder Serverinstanz erstellt, sodass im Falle eines Hardwareausfalls in kalkulierbarer Zeit ein Recovery des vorherigen Betriebszustands hergestellt werden kann. Für eine ordnungsgemäße Wiederherstellbarkeit eines betriebsfähigen Zustands der operativen IT-Systeme (nicht nur der Daten) ist daher immer die Datensicherung auf inhaltlicher Ebene (Daten) und die Abbildsicherung auf technischer Ebene zu beachten und beides durchzuführen.
Diese Prozesse werden standardmäßig im dvo Rechenzentrum abgebildet.

4 Tägliches Monitoring / Überwachung des Backups / eventuelle Fehlerbehebung

Der Sicherungsstatus eines jeden Backup-Auftrags wird täglich automatisiert durchgeführt.
Für die auf Basis des Monitorings erkannten Probleme werden die jeweils notwendigen Maßnahmen automatisiert eingeleitet und gemäß der allgemeinen Interventionszeit erbracht.
Der Auftraggeber erhält keine weiteren Informationen zur Datensicherung, da sie in jedem Service des dvo Rechenzentrums enthalten ist und als Hintergrundprozess fungiert.

5 Interventionszeiten und Definition von kritischen Backupfehlern, Erfolg und unkritischen Backupfehlern
Als kritisch wird ein Backup-Problem eingestuft, wenn das letzte erfolgreiche Backup eines Systems älter als einen Arbeitstag ist.
Ein erfolgreiches Backup im Sinne dieser Leistungsbeschreibung liegt vor, wenn die Log-Dateien der jeweiligen Datensicherungssoftware den Status "erfolgreich" anzeigen.
Bei kritischen Problemen wird seitens Auftragnehmer innerhalb von vier Stunden während des Servicezeitraums Mo-Do 8-17 Uhr und Fr 8-14 Uhr mit der Problemlösung innerhalb der eigenen Rechenzentrums-Infrastruktur begonnen.
Die Interventionszeit beginnt mit der automatisierten Mitteilung an den Auftragnehmer per Online-Ticketing-System und läuft während des oben erwähnten Servicezeitraums.
Bei unkritischen Problemen – einzelne Dateien bzw. E-Mails können aufgrund von Datei- oder Zugriffsfehlern im Augenblick nicht gesichert werden - muss innerhalb von 48 Stunden während des Servicezeitraums Mo-Do 8-17 Uhr und Fr 8-14 Uhr mit der Problemlösung oder Terminierung der Problemlösung begonnen werden.

6 Periodische, manuelle Testrücksicherung von ausgewählten Ordnern
Es erfolgt periodisch (quartalsweise) eine stichprobenartige Datenrücksicherung von ausgewählten Dateien.
Die Rücksicherung erfolgt auf einen vom Auftragnehmer gewählten temporären Datenspeicherungs-Ort innerhalb der dvo Rechenzentrums-Umgebung.
Nach der Rücksicherung erfolgt die Durchführung eines durch die Backup-Software vorgenommenen Binär-Vergleich der auf dem Sicherungsdatenträger vorhandenen Daten mit den auf dem Quelldatenträger vorhandenen Daten. Bei einer etwaigen Abweichung laut Ergebnis der Backup-Software erfolgt eine Analyse mit darauf folgenden Maßnahmenplan.
Die Umsetzung des Maßnahmenplans erfolgt eigenständig durch den Auftragnehmer bis zur erfolgreichen Wiederherstellbarkeit der Daten. Es wird die Standard-Interventionszeit angewandt.

7 Durchführung einer Disaster-Recovery-Simulation eines Systems („Feuerwehrübung“)
Es erfolgt periodisch (jährlich) eine stichprobenartige Wiederherstellung eines vom Auftragnehmer bestimmten Serversystems innerhalb der dvo Rechenzentrumsumgebung. Der Erfolg der stichprobenartigen Wiederherstellung wird auf Basis eines Client-Zugriffs auf die auf dem Server liegenden Daten/Applikationen festgestellt.

8 Überprüfung / Aktualisierung des Datensicherung-Notfallplans
Es erfolgt eine periodische (jährlich) Prüfung auf Stimmigkeit/Konsistenz des Plans in sich und in Bezug auf die mit den Backup-Systemen zu sichernden Daten.
Zur Prüfung wird eine interne Auflistung über die als notfallplan-relevanten Daten/Applikationen/Systeme/Dienste des dvo Rechenzentrums herangezogen. Bei einer etwaigen Abweichung erfolgt eine Aktualisierung des Notfallplans durch den Auftragnehmer.
Der Notfallplan sowie die zugrunde liegende Auflistung ist als vertrauliches, internes Dokument klassifiziert und wird Dritten aus Sicherheits- und Datenschutzgründen nicht zugänglich gemacht.

IV Datenlöschung und Aufbewahrungsfrist

1 Aufbewahrungsfrist

Es wird die Handhabung von direkten Benutzerdaten, Log- und Monitoring-Daten sowie gesicherten und replizierten Daten unterschieden:

Für direkte Kunden- bzw. Benutzerdaten ist – unabhängig von den gebuchten Services – eine Aufbewahrungsfrist von maximal 6 Monaten ab Deaktivierung des bzw. der Kundenaccounts vorgesehen. Abhängig vom gebuchten Service kann die Datenlöschung auf Wunsch auch früher bzw. direkt mit Erreichen der Kündigungsfrist erfolgen. Diese Möglichkeit ist aber vom gebuchten Rechenzentrums-Produkt (Service) abhängig, da nicht bei jedem Produkt die Möglichkeit einer architektonisch völlig unabhängigen Datenlöschung besteht.
Siehe dazu die Leistungsbeschreibungen der einzelnen Produkte.

Für Log- und Monitoring-Daten ist eine maximale Aufbewahrungsfrist von 2 Jahren vorgesehen, um technische Analysen der Systemperformance, Auslastungen sowie anderer technisch relevanter Parameter vornehmen zu können, welche ausschließlich der weiteren technischen Verbesserung und dem weiteren technischen Ausbau der dvo Rechenzentrumsstandorte dienen.
Diese Daten können nur bei Nutzung einer dedizierten Infrastruktur vorab auf Wunsch entfernt werden, somit ist diese Möglichkeit nur bei dem dvo Rechenzentrums-Produkt „net:center Enterprise“ auf Wunsch möglich.
Log- und Monitoring-Daten enthalten Login- und Rechnernamen sowie Quell-IP-Adressen und ggf. davon unabhängig gespeicherte E-Mail-Adressen keine benutzerbezogenen oder persönlichen Daten.

Für gesicherte Daten gelten die allgemeinen Archivrichtlinien im Kapitel „Datensicherung“ dieses Dokuments. Dies bedeutet, dass gesicherte und physisch aus dem operativen Bereich gelöschte Daten bis zum Ende der Archivrichtlinie (5 Jahre) „hinausaltern“, also zunehmen nur noch auf den ältesten Ständen verfügbar sind.
Die „Hinausalterung“ kann nur bei Nutzung einer dedizierten Infrastruktur auf Wunsch entfallen, somit ist diese Möglichkeit nur bei dem dvo Rechenzentrums-Produkt „net:center Enterprise“ auf Wunsch möglich.

Die Aufbewahrungsfrist von Abbildsicherungen beträgt generell maximal zwei Monate.

Bei replizierten Daten findet keine Versionierung bzw. Archivierung statt, sodass gelöschte Daten nach spätestens einem Tag auch im Replikat des jeweils anderen dvo Rechenzentrum-Standorts entfernt wurden.

2 Datenlöschung

Es wird, wie bereits bei der Aufbewahrungsfrist erwähnt, die Handhabung von direkten Benutzerdaten, Log- und Monitoring-Daten sowie gesicherten und replizierten Daten unterschieden:

Für direkte Kunden- bzw. Benutzerdaten wird die Datenlöschung je nach gebuchtem Produkt des dvo Rechenzentrums (Service) entweder automatisiert bei bzw. nach Deaktivieren bzw. Löschen des Kundenaccounts oder manuell vorgenommen.
Abhängig vom gebuchten Service kann die Datenlöschung auf Wunsch auch früher bzw. direkt mit Erreichen der Kündigungsfrist erfolgen. Diese Möglichkeit ist aber vom gebuchten Rechenzentrums-Produkt (Service) abhängig, da nicht bei jedem Produkt die Möglichkeit einer architektonisch völlig unabhängigen Datenlöschung besteht. Sonst gilt die Aufbewahrungsfrist aus Punkt 1.
Siehe dazu die Leistungsbeschreibungen der einzelnen Produkte.

Für Log- und Monitoring-Daten findet die Datenlöschung automatisiert gemäß der Aufbewahrungsfrist aus Punkt 1 statt.

Für gesicherte Daten gelten die allgemeinen Archivrichtlinien im Kapitel „Datensicherung“ dieses Dokuments. Eine Löschung bestimmter, einzelner Daten aus servicespezifischen oder übergreifenden Sicherungssätzen über alle Archivstände hinweg ist derzeit bei gängigen bzw. marktüblichen Backupsoftware-Lösungen nicht möglich,

weshalb ein „Hinausaltern“ der gesicherten Daten stattfindet.
Die „Hinausalterung“ kann nur bei Nutzung einer dedizierten Infrastruktur auf Wunsch entfallen, somit ist diese Möglichkeit nur bei dem dvo Rechenzentrums-Produkt „net:center Enterprise“ auf Wunsch möglich.

Abbildsicherungen sind in einen vollautomatisierten Zyklus eingebunden, ein manueller Eingriff in Form der Löschung bestimmter Abbildsicherungen oder Daten daraus wird im Sinne der Gewährleistung der Verfügbarkeitsqualität aller operativen Systeme im dvo Rechenzentrum grundsätzlich nicht vorgenommen.

Bei replizierten Daten findet – wie bereits in Punkt 1 erwähnt - keine Versionierung bzw. Archivierung statt, sodass gelöschte Daten nach spätestens einem Tag auch im Replikat des jeweils anderen dvo Rechenzentrum-Standorts entfernt wurden. Ein manueller Eingriff ist daher nicht erforderlich bzw. wird nicht durchgeführt.

V **Sicherheit dvo Rechenzentrum**

1 Allgemein

Das dvo Rechenzentrum ist an beiden Standorten mit einer hochwertigen Enterprise-Sicherheits-Infrastruktur von namhaften, internationalen Herstellern ausgestattet, die allen gängigen Branchen- und Industrie-Standards sowie dem Stand der Technik entspricht.
Erweiterte Infrastrukturkomponenten und Techniken sollen den Betrieb darüber hinaus langfristig gegen eine Vielzahl von Bedrohungen sichern.
Die Sicherheitsbetrachtung im dvo Rechenzentrum konzentriert sich auf das Zusammenspiel der beiden wesentlichen Aspekte:

- Aktuelle, gewartete und leistungsfähige Enterprise-Hard- und Software
- Meldewesen mit IT- und Incident-Management-System sowie definierten und nachvollziehbaren Interventionszeiten

Einige Kernpunkte der umgesetzten und in Betrieb befindlichen Sicherheitsaspekte sind in den folgenden Punkten aufgeführt und erläutert.

2 Inventarisierung

Es findet eine tägliche automatische Aktualisierung der Auflistung der installierten Hard- und Softwarekomponenten aller relevanten Systeme innerhalb des dvo Rechenzentrum im vom bereitgehaltenen IT-Management-System statt. Mit dem IT-Management-System unterstützt der Auftragnehmer die infrastrukturellen, sicherheitstechnischen und qualitätssichernden Leistungen des dvo Rechenzentrums.
Bei auftretenden Störungen oder Unstimmigkeiten im IT-Management-System wird eine Problemlösung nach üblichen Standards herbeigeführt.

3 Anti-Virus Einsatz im Rechenzentrum:

Der auf entsprechenden Frontend-Systemen betriebene Managed Anti-Virus beinhaltet die Bereitstellung von Lizenzen inklusive Wartungs-/Updatepakete durch den Auftragnehmer für einen Schadsoftware-Schutz der jeweiligen Services. Managed Anti-Virus bedeutet in diesem Zusammenhang die Sicherstellung und regelmäßige Überprüfung, dass ein aktueller Virenscanner bei den entsprechenden Server-Systemen im Einsatz ist.
Dies erfolgt über die Prüfung der Aktualität der vom Softwarehersteller bereitgestellten Signaturen täglich und es erfolgt eine Alarmierung der technischen Serviceabteilung des Auftragnehmers, sobald eine Signatur älter als 2 Kalendertage sein sollte. Zusätzlich werden die gefundenen Viren in eine Quarantäne eingestellt und dann durch einen Techniker des Auftragnehmers interpretiert.
Im Anschluss wird der Techniker – sofern sinnvoll und erforderlich bzw. je nach gebuchtem Service - innerhalb der Interventionszeit nach Kapitel I Punkt 8 dem Kunden einen Vorschlag unterbreiten, ob die infizierte Datei gelöscht oder zurück in den Produktivbetrieb gebracht werden soll. Der Kunde wird hierzu eine kurze E-Mail mit seinem Wunsch an den Auftragnehmer übermitteln. Gegebenenfalls erfolgt dieser Vorgang auch in direkter Kommunikation.
Ein 100%iger Anti-Virus-Schutz ist nicht möglich. Der Auftragnehmer wird mittels des genannten Standard-Antivirus-Programms zum Schutz der Rechenzentrumsumgebung beitragen und die Aktualität sowie das Laufverhalten überprüfen.
Weitere implementierte Schutzmechanismen für Rechenzentrums-Services werden in anderen Teilen dieses Dokuments ausgeführt.

4 Web-Filter/Webseiten-Sicherheit

Es wird ein mehrstufiges Web-Filter-System für relevante Services im dvo Rechenzentrum über das IT-Management-System bzw. die zentrale Firewalling-Infrastruktur zur Verfügung gestellt. Es enthält Funktionen, welche nach Standard-Vorgaben unsichere Seiten nach vorbereiteten und redaktionell gepflegten Kategorien sperrt, automatisierte White- & Black-List-Einträge auf Basis von dynamischen Filterlisten setzt sowie die am häufigsten besuchten Webseiten aus Gründen der sicherheitstechnischen Überwachung anonymisiert

analysiert. Die systemtechnische Umsetzung und laufende Wartung wird von Auftragnehmer global nach Standards und Erfahrungswerten durchgeführt.
Ein 100%iger Schutz vor dem Zugriff auf schadhafte Webseiten ist nicht möglich. Der Auftragnehmer wird nach den üblichen Standards weitere und laufende Maßnahmen zur Webseiten-Sicherheit durchführen und überprüfen.

5 Installation/Verteilung aktueller Sicherheitsupdates - Patchmanagement
Installation aktueller Microsoft- und Drittanbieter-Sicherheitsupdates auf operativer Betriebssystemebene im gesamten dvo Rechenzentrum. Nach Installation eines Updates ist häufig ein Neustart der Server notwendig. Dieser wird ohne Absprache außerhalb der Arbeits- bzw. Verfügbarkeitszeit (Mo-Do 8-17 Uhr und Fr 8-14 Uhr) und in der Regel in den Nachtstunden am Wochenende (Sa 0-6 Uhr, So 22-6 Uhr) ausgeführt und ist Bestandteil des jeweiligen Service. Die Sicherstellung der erfolgreichen Installation der Sicherheitsupdates erfolgt über eine Abfrageroutine mit automatischen Meldewesen.
Der Auftragnehmer stellt die Updates in 95% der Fälle innerhalb von 2 Wochen, in 99% der Fälle innerhalb von 3 Wochen nach Erscheinen der Updates für die Server des Kunden bereit. Maßgebend für die Ermittlung des prozentualen Erfolgs ist der aus dem vom Auftragnehmer bereitgestellten Management-System abrufbare Bericht, der der für interne Qualitätssicherungs- und Überprüfungszwecke genutzt wird. Der Auftragnehmer wird die vom Softwarehersteller veröffentlichten Patches ohne vorherige, explizite Prüfung in mehreren Ausrollungsschritten auf den entsprechenden Systemen im dvo Rechenzentrum installieren.
Standardmäßig werden jedoch neu hinzukommende Patches global überprüft und erst einige Tage nach Erscheinen ausgeliefert, um anfängliche Probleme mit neuen Patches minimieren zu können.

Die Haftung für die Fehlerfreiheit der Sicherheitsupdates, die Sinnhaftigkeit der Risiko-Klassifizierung sowie die Kompatibilitätseinschätzung mit der zu aktualisierenden Software liegt allein beim jeweiligen Softwarehersteller. Dem Kunden ist bewusst, dass Sicherheitsaktualisierungen Veränderungen an der installierten Software vornehmen, um die Sicherheit oder Stabilität zu verbessern. Bei diesen Veränderungen kann es zu Problemen kommen, die die Lauffähigkeit des Systems negativ beeinflussen. Für Folgeschäden aus diesem Umstand kann der Auftragnehmer keine Haftung übernehmen, jedoch wird er eine Problemlösung nach üblichen Standards mithilfe des Supports des jeweiligen Drittanbieters herbeiführen.
Es gilt die Standard-Interventionszeit oder für kritische Probleme die verkürzte Interventionszeit.
Bei Problemen in Kombination mit individuell eingesetzten oder angepassten Drittanbieter-Softwareprodukten behält sich der Auftragnehmer vor, die Herbeiführung der Problemlösung nach Kapitel I Punkt 10 in Rechnung zu stellen.

6 Firmwareupdates
Bei Infrastruktur-Geräten, welche keine automatisierte Überprüfung und Installation von Firmware-Updates zulassen, wird monatlich bzw. quartalsweise kontrolliert, ob es ein neues Update der jeweiligen Firmware zur Verfügung steht. Die Installation wird später zu einem definierten Wartungsfenster manuell oder automatisch installiert, das jeweilige Gerät danach neu gestartet. Im Anschluss an den Neustart findet eine allgemeine Funktionskontrolle statt und die Verbindung zum Managementsystem des Auftragnehmers wird reinitialisiert.

7 Zentrale Firewalling-Infrastruktur
Im dvo Rechenzentrum kommt eine hochverfügbare und hochperformante Enterprise-Firewalling-Infrastruktur zum Einsatz, welche die zentrale Verbindungsverwaltung aller dvo Rechenzentrumsprodukte (Services) darstellt. Neben feingliedriger Netzwerksegmentierung werden ausschließlich Access-Control-Listen auf Basis einer Standard-Verweigerungs-Richtlinie angewandt und ausschließlich verschlüsselte Verbindungen eingehend zugelassen bzw. gewährleistet.
Über netzwerk- und routingtechnische Funktionalitäten hinaus sind feingliedrige Einbruchsschutz-, Antivirus-, Malware- und Applikations-Kontroll-Regeln für alle Netzwerksegmente im Einsatz, die den Netzwerkverkehr während des Durchflusses analysieren, ggf. blocken und an das IT-Management-System melden.
Für relevante Netzwerksegmente und dvo Rechenzentrums-Produkte (Services) wird darüber hinaus verschlüsselter Datenverkehr nach oben genannten Kriterien analysiert und eine Sandboxing-Lösung eingesetzt, die unbekannte Dateien in einer virtuellen Umgebung testweise ausführt, um sicherzustellen, dass sie schadfrei sind, bevor sie an den Bestimmungsort weitergeleitet werden.

Zusätzlich eingesetzte und gewartete Webfilter werden im Punkt „Web-Filter/Webseiten-Sicherheit“ erwähnt.

Das eingesetzte Management-System gewährleistet mehrmals täglich eine automatisierte Ausbringung aller sicherheitstechnisch relevanter Signaturen, Listen, Patches und Softwareupdates auf die Firewalling-Infrastruktur und überprüft den Erfolg der Ausrollung. Bei Fehlern erfolgt eine sofortige Meldung in das IT-Management-System des Auftragnehmers, der eine Problemlösung nach üblichen Standards unter Bedacht der kommunizierten Interventionszeit herbeiführen wird.
Ebenso meldet die Firewalling-Infrastruktur erkannte Probleme, Einbruchsversuche, erkannte Schadsoftware oder ungewöhnliches Netzwerkverhalten in das IT-Management-System des Auftragnehmers, der eine Analyse und ggf. eine Problemlösung nach üblichen Standards innerhalb der kommunizierten Interventionszeit herbeiführen wird.

8 Verbindungssicherheit/Verschlüsselung/HTTPS-Filter-Proxy
Zusätzlich zur bereits genannten Firewalling-Infrastruktur ist eine hochverfügbare, intelligente Enterprise-HTTPS-Filter-Proxy-Infrastruktur im Einsatz, welche für alle dvo Rechenzentrums-Produkte (Services) mit zentralem Portaleinstieg genutzt wird und drei Hauptaufgaben erfüllt:

- Gewährleistung eines hohen Verschlüsselungs- und Verbindungssicherheitsstandards (A+ Rating bei Überprüfungs- bzw. Penetrations-Tests)
- Sicherheitstechnische Entkoppelung der operativen Hintergrund-Infrastruktur zum erweiterten Schutz der Daten und Zugangskennungen.
- Erweiterter Lastenausgleich und Ausfallsschutz durch doppelte redundante Auslegung sowohl der HTTPS-Filter-Proxy-Infrastruktur als auch der operativen Hintergrund-Infrastruktur für alle relevanten Services im dvo Rechenzentrum.

9 Monitoring, Alarmierung und Incident Management
Überwachung der Firewalling-Infrastruktur, anderer Sicherheitsinfrastruktur und der Internetanbindungen rund um die Uhr hinsichtlich der Erreichbarkeit/Internetverbindung/Bandbreite, Lauffähigkeit der Firewall-Dienste, Aktualität der Anti-Virus-Signaturen, Aktualität der Intrusion Prevention, Webfilter und anderer Sicherheitsdienste (wie bereits im Punkt Zentrale Firewalling-Infrastruktur beschrieben), physischer Zustand der Hardware inkl. Prozessorauslastung, Connection-Zahl im Hinblick auf Auslastung sowie hinsichtlich anderer relevanter Parameter.
Für etwaige Probleme, die einen Eingriff rechtfertigen und die mit dem Monitoring erkannt werden, gilt die jeweils anzuwendende, kommunizierte Interventionszeit, unter deren Bedacht der Auftragnehmer eine Analyse und ggf. Problemlösung nach üblichen Standards herbeiführen wird.
Meldungen der Sicherheitsinfrastruktur werden von technischen Mitarbeitern des Auftragnehmers interpretiert und als Vorfall (Incident) im Management-System erfasst. Ggf. wird ein Incident-Response-Plan je nach Schwere und Tragweite des möglichen Vorfalls (Incident) ausgeführt, der geeignete Maßnahmen vorsieht.

Der Incident Management Prozess – hier im Speziellen der Major Incident Management Prozess des Auftragnehmers sieht die zentrale und einheitliche Kommunikation von allgemeinen Ereignissen und Vorfällen zu bereitgestellten Cloud Produkten aus Sicht des Auftragnehmers (Servicebetreibers) bzw. ausschließlich aus dessen Sphäre vor und nutzt dazu gegenüber dem Auftraggeber ausschließlich einen Dienst, welcher über eine Service Status Webseite inkl. optional nutzbaren, proaktiven Benachrichtigungsfunktionen abgebildet ist.
Es erfolgt ausdrücklich keine Berücksichtigung bzw. Betrachtung von technischen Problemen bzw. Einschränkungen Dritter.
Das Whitepaper „dvo Service Status - Beschreibung und Nutzung“ steht dem Auftraggeber dabei in der jeweils aktuellen Version für alle Detailinformationen dazu in dessen geschütztem Kundenbereich zur Verfügung.
Der oben beschriebene dvo Service Status Dienst dient ausdrücklich nicht der Kommunikation von Sicherheits- bzw. Datenschutzvorfällen (Data Breaches) im Sinne der EU-DSGVO (Art 34), sondern bildet den allgemeinen, operativen Verfügbarkeitsstatus des jeweiligen Cloud Dienstes ab.

10 Physischer Schutz der Infrastruktur

Der physische Zutritt zu beiden Gebäudestandorten des dvo Rechenzentrums ist mittels digitalem Mehrfaktor-Authentifizierungssystem, mehreren Schleusen und durchgängiger Videoüberwachung gesichert.
State-of-the-Art Klimatisierung und CO2-Brandschutztechnik sichert den Betrieb der Infrastrukturgeräte.

VI Architektur und Verfügbarkeitsmaßnahmen dvo Rechenzentrum

1 Allgemein

Es handelt sich beim dvo Rechenzentrum um ein modulares und auf mehreren Ebenen vollredundantes Architekturdesign. Der besseren Erkennbarkeit halber ist die Architektur im Hinblick auf Verfügbarkeit am Anschluss grafisch dargestellt. Die einzelnen Ebenen werden nach der technischen Reihenfolge der implementierten Verfügbarkeitsmaßnahmen beschrieben.

2 Standorte und physische Gebäuderedundanz

Das dvo Rechenzentrum verfügt über zwei geographisch distanzierte Standorte in Wien und Oberösterreich, die beide eine hohe Verfügbarkeit und Nähe zu Internet-Knotenpunkten besitzen und damit eine hohe Leitungsqualität und niedrige Ausfallsquote bieten. Die Internetanbindungen sind konsequent auf Glasfaser-Basis realisiert und innerhalb der Gebäude mehrfach redundant geführt. Im Falle des Ausfalls eines Leitungsstrangs findet eine Umschaltung vollautomatisiert statt.
Die Stromversorgung an beiden Standorten ist zwei- bis mehrfachredundant von unterschiedlichen Energieanbietern geführt, zusätzlich sind an beiden Standorten ausreichend dimensionierte und gewartete Notstromversorgungen in Form von Diesel-Aggregaten im Einsatz.
Die Standorte sind im Hinblick auf ihre Sicherheits- und Verfügbarkeitsmaßnahmen sowie deren Einhaltung und Wartung zertifiziert.

3 Redundante und transferierbare Internetanbindungen

Am Rechenzentrumsstandort Wien ist die Internetanbindung von zwei technologisch sehr unterschiedlich arbeitenden Anbietern vollredundant ausgeführt, was nicht nur einen Ausfallschutz (auch bei ungerichteten DDoS-Attacken wirksam), sondern auch einen Lastenausgleich bietet (beide Leitungen sind immer aktiv).
Am Rechenzentrumsstandort Oberösterreich ist die Internetanbindung einfach redundant ausgeführt, das bedeutet, dass eine Leitungsredundanz von einer Anbieter-Infrastruktur gewährleistet wird.
Die Routing-Architektur an beiden Standorten ist in einer Form gestaltet, die es ermöglicht, den Datenverkehr vom ursprünglichen Standort auf den jeweils anderen Standort ohne Zeitverlust umzuschalten. (transferierbare Internetanbindung) Diese Funktion ist eine Basis für Standortunabhängigkeit und ein Schlüssel für einen standort-unabhängigen Disaster-Recovery-Notfallplan.
Die Leitungsanbindungen und das zugehörige Routing ist nach Industrie-Standards ausgeführt.

4 Vollredundante Netzwerk- und Sicherheitsinfrastruktur

An beiden Rechenzentrumsstandorten ist die vollständige Sicherheits- und Netzwerkinfrastruktur - unabhängig voneinander - vollredundant gestaltet und nach Industrie-Standards implementiert.
Bei Ausfall eines Geräts erfolgt eine nahtlose und vollautomatische Übernahme des Datenverkehrs auf das Ersatz- bzw. Redundanzgerät. (Stateful-Failover)

5 Speicher-Cluster und vollredundante virtuelle Infrastruktur

Die Virtualisierungsinfrastruktur ist an beiden Rechenzentrumsstandorten in gleicher Weise vollredundant und modular ausgeführt. Die physische Trennung von Datenspeicher- und Rechenkapazitäten (Storage und Server) erlaubt vollständigen und vollautomatisierten Lastenausgleich und Ausfallschutz auf beiden Ebenen.
Der Betrieb der Virtualisierungsinfrastruktur erfolgt nach Industrie-Standards und Best-Practice-Empfehlungen der jeweiligen Soft- bzw. Hardwareanbieter.

6 Storage-Replikation und Disaster Recovery Notfallplan
Die in Punkt 5 bereits erwähnten Datenspeicherkapazitäten (Storage) sind an beiden Standorten in gleicher Weise und modular ausgeführt. Die einzelnen Speicherbereiche (Volumes) der operativ betriebenen Datenspeicher werden kontinuierlich – mehrmals täglich – an den jeweils anderen Rechenzentrumsstandort übertragen, sodass zu jeder Zeit ein vollständiges Abbild der Volumes am jeweils anderen Rechenzentrumsstandort existiert. (Replikation)
Die genannte Funktion (Replikation) ist ein maßgeblicher Schlüssel für den standortunabhängigen Betrieb der dvo Rechenzentrums-Produkte (Services) in einem Notfall-Szenario, in dem ein Rechenzentrums-Standort längerfristig aus unterschiedlichen Gründen vollständig ausfällt. Gemeinsam mit der im Punkt 3 erwähnten, transferierbaren Internetanbindung wird ein Disaster-Recovery-Szenario möglich, das den Fortbetrieb der dvo Rechenzentrums-Produkte (Services) mit allen zugehörigen Daten erlaubt.
Die Replikations- und Inbetriebnahme-Vorgänge erfolgen nach Industrie-Standards und Best-Practice-Empfehlungen der jeweiligen Soft- bzw. Hardwareanbieter.
Dieses Szenario ist im Disaster-Recovery-Notfallplan prozessual festgehalten. Der Disaster-Recovery-Notfallplan ist aufgrund seiner sicherheitstechnischen Inhalte ein vertrauliches, internes Dokument und wird Dritten nicht zur Verfügung gestellt.
In der derzeitigen Implementierungsstufe wurden bei Inkrafttreten des Disaster-Recovery-Notfallplans folgende Einschränkungen für den Betrieb evaluiert:

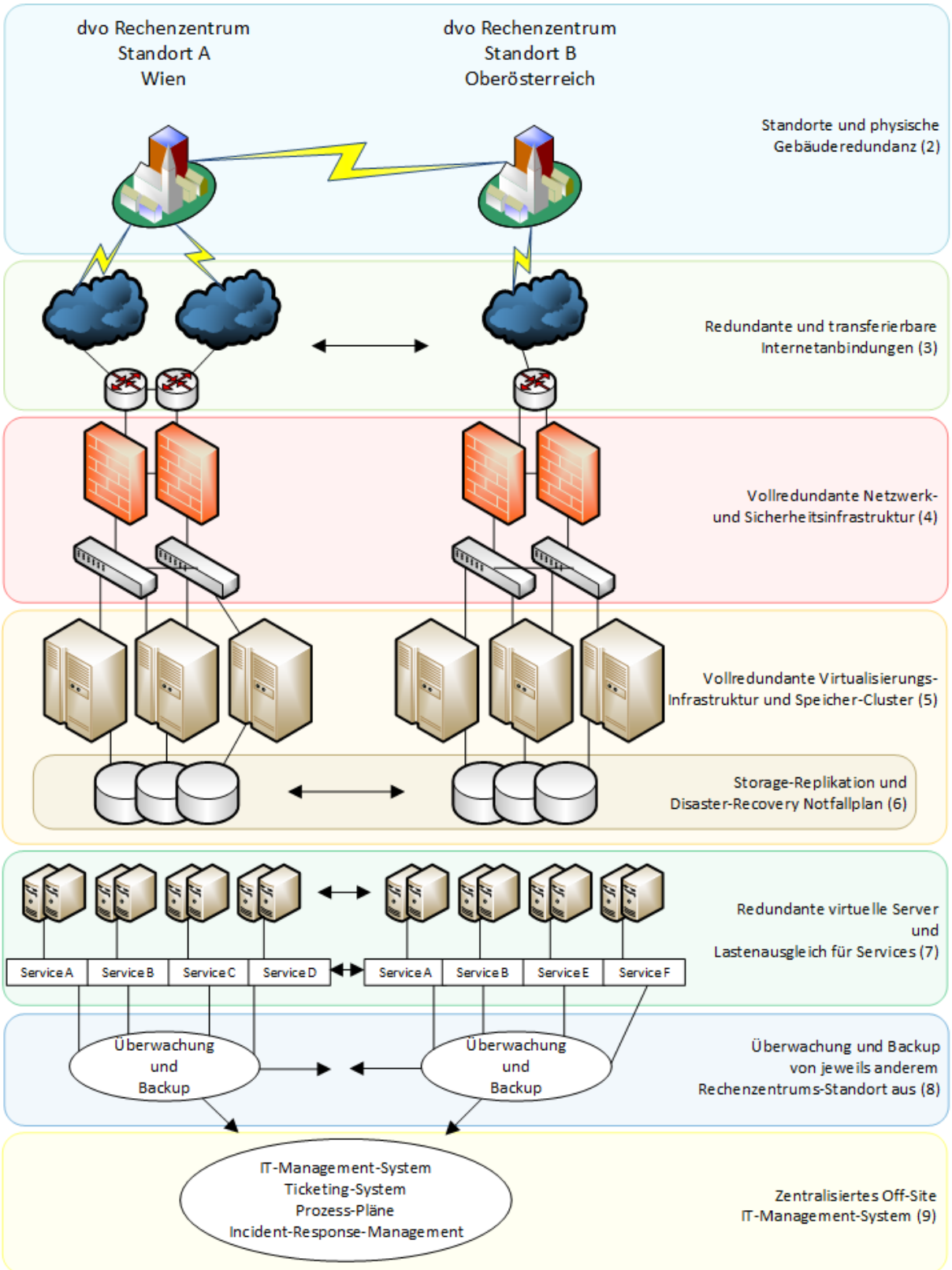
- 4 Stunden Ausfallzeit für Status-Analyse und Entscheidung für Einleiten des Notfallplans
- 16 Stunden Ausfallzeit für Inbetriebnahme wesentlicher Dienste auf anderem Rechenzentrums-Standort
- Verlust von eingegangenen, eingegebenen oder verarbeiteten Daten der letzten fünf Stunden (maximal) vor Beginn des Totalausfalls. Es handelt sich um die Daten, die vor dem Ausfall nicht mehr erfolgreich an den anderen Standort repliziert werden konnten.

7 Redundante virtuelle Server und Lastenausgleich für Services
Auf Ebene der virtuellen Server bzw. der operativen Datenverarbeitung werden auf Produktebene intensiv genutzte oder quantitativ stark angefragte Dienste für einen weiteren Ausfallschutz oder/und zu Lastenausgleichszwecken redundant geführt.
Auf dieser Ebene findet auch die im Kapitel „Datensicherung“ bereits ausgeführte Abbildsicherung der operativen Systeme als auch die konventionelle Datensicherung dieser Systeme statt. Diese werden aus strukturellen Gründen im Punkt 8 ausgeführt.

8 Monitoring und Backup von jeweils anderem Rechenzentrums-Standort
Die Überwachung der infrastrukturellen und operativen Systeme erfolgt vom jeweils anderen Rechenzentrumsstandort aus, um die Erreichbarkeit und Verfügbarkeit der Systeme, Dienste und Produktbestandteile mitüberwachen zu können. Die Überwachungssysteme melden Ereignisse automatisiert an das zentralisierte IT-Management-System.
Die im Kapitel „Datensicherung“ bereits ausgeführte Abbildsicherung der operativen Systeme als auch die konventionelle Datensicherung dieser Systeme ist wie folgt realisiert:
Während die Abbildsicherung am jeweiligen Rechenzentrumsstandort verbleibt, um dort ggf. softwaretechnisch defekt gewordene Systeme binnen zwei bis drei Stunden wiederherstellen zu können, wird die konventionelle Datensicherung aus Ausfalls- und Verfügbarkeitsgründen auf den jeweils anderen Rechenzentrumsstandort ausgeführt. Eine Wiederherstellung der Daten kann verschlüsselt übertragen oder verschlüsselt per Datenträger erfolgen, die Wiederherstellungszeit ist vollständig von der Größe und Beschaffenheit der Daten abhängig und kann realistisch schwer pauschal geschätzt werden.

9 Zentralisiertes Off-Site IT-Management-System
Das zentralisierte IT-Management- und Ticketing-System beinhaltet Prozesspläne inkl. Incident-Response-Management, erhält Einmeldungen von Kunden als auch der IT-Überwachungssysteme und dient als zentrale Plattform für die Steuerung des Betriebs. Die Implementierung verfolgt Industrie-Standards.

10 Grafische Darstellung Architektur und Verfügbarkeitsmaßnahmen



VII Zusammenfassung technisch-organisatorische Maßnahmen im dvo Rechenzentrum lt. EU-DSGVO bzw. AT-DSAG2018

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
    a. Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen innerhalb des dvo Rechenzentrum, siehe Kapitel V, speziell Punkt 10
    b. Zugangskontrolle: Keine unbefugte Systembenutzung innerhalb des dvo Rechenzentrum durch zwangsweise sichere Kennwörter, automatische Sperrmechanismen ab mehrmaliger Falscheingabe, teilweise mehrstufige Authentifizierung, Verschlüsselung von allen eingehenden Verbindungen;
    c. Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Netzwerk- und Mikrosegmentierung, Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte auf allen Ebenen, Protokollierung von Anmeldungen auf Ebene der Authentifizierung;
    d. Trennungskontrolle: Im Rechenzentrum erfolgt grundsätzlich eine getrennte Verarbeitung von Daten, die in den jeweiligen Bereichen von unterschiedlichen Mandanten und zu unterschiedlichen Zwecken erhoben und verarbeitet wurden, dies wird durch den vollmodularen Aufbau der Architektur und aller Produkte im dvo Rechenzentrum gewährleitet;
    e. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO): Auf Ebene der Speicherung aller Daten innerhalb des dvo Rechenzentrum erfolgt die Ablage ausschließlich modular auf dedizierte Enterprise-Storagesysteme, welche die aufgenommenen Daten ausschließlich auf Blockebene ablegen, replizieren und assoziieren. Ohne das Heranziehen mehrschichtiger Logikelemente sind die gespeicherten Daten nicht zuordenbar.
    Die Verarbeitung personenbezogener Daten innerhalb von Drittanbieter-Anwenderprogrammen sollte in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen – dies muss jedoch von der entsprechenden Drittanbieter-Software ermöglicht bzw. gewährleistet werden;
2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)
    a. Weitergabekontrolle: Es soll kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport stattfinden können, dies wird bei der Verbindung in das dvo Rechenzentrum ermöglicht durch zwingenden Einsatz von verschlüsselten Verbindungen, Verbindungsaufbau per Virtual Private Networks (VPN), mehrstufige Sicherheitszonen- und Authentifizierungsgestaltung je nach Produkt (siehe LB des Produkts);
    b. Eingabekontrolle: Es soll festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, dies erfolgt z.B. im DMS Online Dokumentenmanagement. Jedoch muss dies von der entsprechenden Drittanbieter-Software ermöglicht bzw. unterstützt werden und ist nicht Bestandteil der gegenständlichen, gehosteten Produkte.
3. Verfügbarkeit und Belastbarkeit (Art.. 32 Abs. 1 lit. b DS-GVO)
    a. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), Stromversorgungsredundanz, Virenschutz, Firewall, Meldewege und Notfallpläne - siehe Inhalte der vorliegenden Leistungsbeschreibung.
    b. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) – siehe Kapitel III dieser LB
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)
    a. Datenschutz-Management: Liegt vor und wird gemäß Auftragsverarbeiter-Vereinbarung verwaltet.
    b. Incident-Response-Management: Liegt vor, siehe Kapitel V Punkt 9.
    c. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO); Dies muss ausschließlich von der entsprechenden Drittanbieter-Software ermöglicht bzw. unterstützt werden.
    d. Auftragskontrolle: Es erfolgt keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B. durch eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl von Drittanbietern und ggf. Sub-Dienstleistern, Vorabüberzeugung, Nachkontrollen.

Anlage 1 – Liste standardmäßig gewarteten und im Rahmen der dvo Rechenzentrums-Produkte abgedeckten Anwendungen & Dienste

Die Flatrate ist gültig für die im Folgenden genannten Anwendungen & Dienste sofern die Flatrate für den jeweiligen Server gebucht ist, auf dem die nachfolgenden Anwendungen & Dienste betrieben werden.

- Anwendungen & Dienste des Betriebssystems: ActiveDirectory, DNS, DHCP, Lizenzdienst.
- Microsoft Druckdienste
- Microsoft Filedienste
- Microsoft Exchange-Server
- Microsoft Terminal Services (Remote Desktop Services)
- Citrix XenApp oder XenApp Fundamentals sowie Citrix Receiver Clients bei net:center Produkten
- Thinprint Infrastruktur bei net:center Enterprise
- VMware vSphere
- Microsoft Office
- Adobe Reader
- Mozilla Firefox
- dvo Software

Ausgeschlossen sind nicht genannte Drittanbieter-Anwendungen & -Dienste die mit den vorgenannten Anwendungen und Dienste verknüpft sind, auch wenn diese augenscheinlich zur Applikation gehören.

Anlage 2 – Liste der unterstützten Software für das Patch-Management

Die nachfolgende Liste gilt per Stand 01.01.2018. Der Auftragnehmer behält sich eine Änderung der Listen jederzeit vor.

Liste der unterstützten Microsoft-Software für das Patch-Management

- ASP.NET Web and Data Frameworks
- Active Directory
- Antigen
- Bing
- BizTalk Server
- Developer Tools, Runtimes, and Redistributables
- Device Health
- Exchange
- Expression
- Forefront
- HPC Pack
- Internet Security and Acceleration Server
- Microsoft Application Virtualization
- Microsoft Azure
- Microsoft BitLocker Administration and Monitoring
- Microsoft Dynamics CRM
- Microsoft HealthVault
- Microsoft Lync Server and Microsoft Lync
- Microsoft Online Services
- Microsoft Research AutoCollage
- Microsoft SQL Server PowerPivot for Excel
- Microsoft StreamInsight
- Microsoft System Center Data Protection Manager
- Office
- Office Communications Server And Office Communicator
- Office Live
- SDK Components
- SQL Server
- Silverlight
- Skype
- System Center
- System Center Online
- System Center Virtual Machine Manager
- Systems Management Server
- Virtual Server
- Windows
- Windows Azure Pack
- Windows Azure Pack - Web Sites
- Windows Essential Business Server
- Windows Live
- Windows Small Business Server

Nur Versionsstände der o. g. Microsoft-Software werden unterstützt, welche sich laut Microsoft in der Mainstream-Support oder Extended Support-Phase befinden.

Liste der unterstützten Drittanbieter-Software für das Patch-Management

- **Apple Incorporated**
  - Apple QuickTime
  - Apple iTunes
  - Apple Safari
- **Adobe Systems Incorporated**
  - Adobe Reader
  - Adobe Acrobat
  - Adobe Flash Player
  - Adobe Shockwave Player
  - Adobe Air
- **Don Ho**
  - Notepad++
- **Foxit Corporation**
  - Foxit Reader
- **Google**
  - Google Chrome *
  - Google Earth
- **Mozilla**
  - Mozilla Firefox
  - Mozilla Firefox ESR
  - Mozilla Thunderbird
  - Mozilla Thunderbird ESR
  - Mozilla SeaMonkey
- **Opera Software ASA**
  - Opera Browser
  - Opera Cromium
- **Oracle Corporation**
  - Java Runtime Environment
- **RARLAB**
  - WinRAR
- **Skype Limited / Microsoft**

- Skype
- **VideoLAN**
  - VLC
- **WinZip Computing**
  - WinZip

Nur Versionsstände der o. g. Drittanbieter-Software werden unterstützt, für welche laut jeweiligem Hersteller kostenlose Patches angeboten werden.