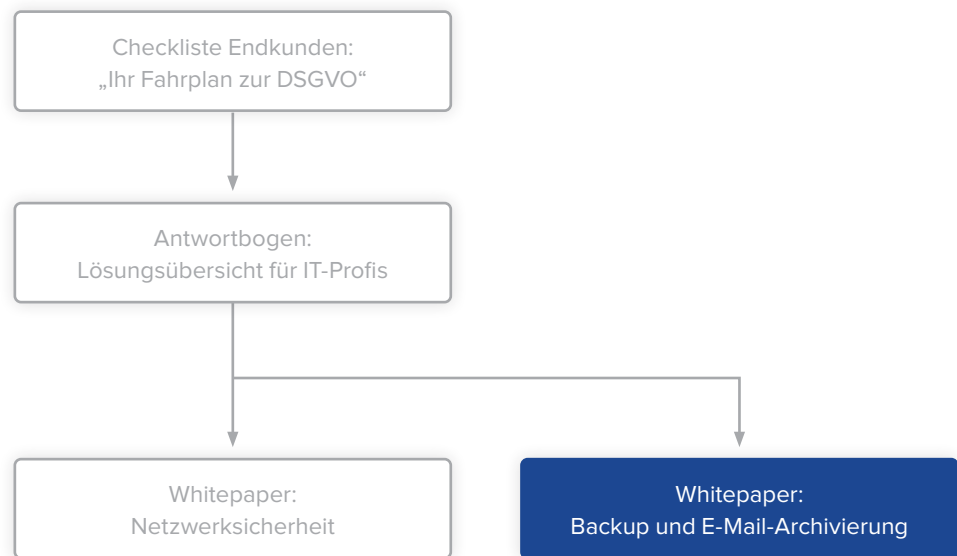


Themenserie DSGVO: Backup und E-Mail- Archivierung

Die Themenserie zur DSGVO im Überblick

Hier finden Sie alle unsere Materialien zur DSGVO zu einem Workflow sortiert, damit Sie Ihre Kunden bestmöglich auf die DSGVO vorbereiten und proaktiv die Projektplanung beginnen können:





Vorwort

Am 25. Mai 2018 trat die EU-Datenschutz-Grundverordnung (DSGVO) vollumfänglich in Kraft. Verstöße gegen die DSGVO können empfindlich hohe Strafen nach sich ziehen – damit sind Ihre Kunden unter Zugzwang, den Umgang mit personenbezogenen Daten auf den Prüfstand zu stellen und Prozesse rechtlich neu zu ordnen. Das betrifft auch die gesamte IT-Infrastruktur, von Mechanismen der Netzwerksicherheit über System-Management bis hin zu Backups- und E-Mail-Archivierungssystemen.

Inhalt

1.	Einleitung	5
2.	Artikel 32: Sicherheit der Verarbeitung	6
3.	Von der gesetzlichen Theorie zur technischen Umsetzung: der Backup-Plan	7
4.	Die Umsetzung: Lösungen für Sie als IT-Profi	9
4.1	Altaro – VM Backup für Hyper-V und VMware	11
4.2	BackupAssist – führend bei Windows-Server-Backup	12
4.3	OpenText Cybersecurity – Backup as a Service	13
4.4	Cove Data Protection – Backup & Recovery	14
4.5	MailStore – für rechtssichere E-Mail-Archivierung	15
5.	Das Backup & die DSGVO: Was sind Ihre nächsten Schritte?	16

1. Einleitung

Wir möchten Sie als IT-Profi in der Argumentation und Projektplanung bei Ihren Kunden unterstützen. Daher informieren wir Sie in unserer Whitepaper-Serie zu den für Sie relevantesten – weil technisch umsetzbaren – Artikeln der [DSGVO](#). Der erste Teil unserer Serie beschäftigt sich mit dem Artikel 32 “Sicherheit der Verarbeitung” und erklärt, welche Rolle eine Backup- und Recovery-Strategie sowie das Thema E-Mail-Archivierung in diesem Kontext spielen.

Als IT-Dienstleister stehen Sie dabei vor der Herausforderung, die Möglichkeiten zur Umsetzung der DSGVO zu identifizieren, sie mit den vorhandenen Gegebenheiten in Einklang zu bringen und auf dieser Basis bei Ihren Kunden eine geeignete Sicherheitsstrategie anzubringen. Erschwerend kommt hinzu, dass die Datenschutz-Grundverordnung in ihrer Komplexität nicht mit einer einzigen Lösung, sondern nur aus verschiedenen Ansatzpunkten heraus vollumfänglich umgesetzt werden kann. So können auch technische Maßnahmen nur ein Baustein zur DSGVO-Konformität sein, neben organisatorischen und personellen Prozessen.

In diesem Whitepaper präsentieren wir Ihnen, welche gesetzlichen Rahmenkriterien beim Thema Backup sowie E-Mail-Archivierung zu bedenken sind und welche Lösungen Ihnen dabei zur Verfügung stehen. So können Sie auf einen Blick die passende Strategie für unterschiedlichste Kundenumgebungen aufstellen und die Projektplanung proaktiv angehen.

Die wichtigsten Eckdaten der Datenschutz-Grundverordnung

- Gilt vollumfänglich seit dem 25. Mai 2018
- Betrifft den Umgang mit personenbezogenen Daten (pbD) also “[...] alle(n) Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; [...]” ¹
 - Beispiel: Name, Geburtsdatum, E-Mail- oder IP-Adresse ²
- Betrifft alle Unternehmen, die pbD erheben und verarbeiten
- Gilt unabhängig vom Standort des Unternehmens oder der verarbeitenden Instanz ³
- Bei Verstößen können Bußgelder in Höhe von bis zu 20 Millionen Euro oder 4% des weltweit erzielten Vorjahresumsatzes erhoben werden. ⁴

2. Artikel 32: Sicherheit der Verarbeitung

Ein Backup- und Recovery-Plan ist bereits von sich aus eine organisatorisch sowie unternehmerisch absolut sinnvolle Maßnahme und daher in den meisten Unternehmen gängige Praxis. Nun ergibt sich im Rahmen der DSGVO mit dem [Artikel 32 zur "Sicherheit der Verarbeitung"](#) auch eine gesetzliche Notwendigkeit zur Datensicherung: Denn nach Art. 32 Abs. 1 hat der Verantwortliche – also das Unternehmen, welches die Daten in erster Instanz erhebt – technische und organisatorische Maßnahmen zu treffen, um diese vor Verlust oder Missbrauch zu schützen. Dies muss unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art und Weise der Datenerhebung und Verarbeitung geschehen, was bedeutet: Je sensibler die Daten sind bzw. je größer das Risiko im Falle des Missbrauchs oder Verlustes ist, desto umfassender müssen die Sicherheitsvorkehrungen sein.

Je sensibler die Daten sind bzw. je größer das Risiko im Falle des Missbrauchs oder Verlustes ist, desto umfassender müssen die Sicherheitsvorkehrungen sein.

Ziel der Maßnahmen – und damit im weiterführenden Sinn Zweck der eingesetzten Lösungen – ist es unter anderem auch, "die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme [...] sicherzustellen" (Art. 32 Abs.1 lit b) DSGVO) und die "Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen" (Art. 32, Abs. 1, lit c) DSGVO).⁵ Das bedeutet, dass bei der Wahl der Lösung nicht der tägliche Standard, sondern vielmehr Krisensituationen wie Naturkatastrophen, Hardware-Versagen oder Cyberkriminalität als Maßstab herangezogen werden sollten. Darüber hinaus fordert der Artikel auch ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen. Im Idealfall ist hier ein Information Security Management System nach ISO 27001 im Einsatz, Abhilfe kann jedoch auch eine Protokoll-Funktion schaffen. Darüber hinaus fordert der Artikel auch ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen. Im Idealfall ist hier ein Information Management Security-System nach ISO 27001 im Einsatz, Abhilfe kann jedoch auch eine Protokoll-Funktion schaffen.

Bei der Wahl der Lösung sollten nicht der tägliche Standard, sondern vielmehr Krisensituationen wie Naturkatastrophen, Hardware-Versagen oder Cyberkriminalität als Maßstab herangezogen werden.

Auf einen Blick: Was bedeutet "Sicherheit der Verarbeitung"?

- Die Daten müssen auch im Ernstfall schnellstmöglich wieder verfügbar gemacht werden.
- Die Integrität und Sicherheit der pbD muss nachweislich gewährleistet sein.
- Die getroffenen Maßnahmen sollen auf dem Stand der Technik – also marktfähig – sein.
- Je sensibler die Daten sind, bzw. je größer das Risiko für den Betroffenen bei Verlust oder Manipulation der pbD ist, desto umfassendere Vorkehrungen sind zu treffen.

3. Von der gesetzlichen Theorie zur technischen Umsetzung: der Backup-Plan

In der Praxis spiegeln sich die in Artikel 32 geforderten Maßnahmen in einem krisensicheren Backup- und Recovery-Plan wider, garantiert dieser doch die Verfügbarkeit der Unternehmensdaten auch im Ernstfall. Dabei profitieren Ihre Kunden auch von der Gewissheit, datengetriebene Geschäftsprozesse bestmöglich gegen Ausfallzeiten gesichert zu haben. Sie als IT-Profi können damit eine zweigleisige Argumentationsstruktur aufbauen: mit den Vorteilen in Sachen Unternehmenssicherheit auf der einen und der gesetzlichen Notwendigkeit eines Backups auf der anderen Seite.

Eckpunkte eines DSGVO-konformen Backups

Sie unterstützen Ihre Kunden in Sachen „Nachweisbare DSGVO-Konformität“ umso besser, je transparenter, nachvollziehbarer und granularer eine Lösung arbeitet.

Eine ausfallsichere, verlässliche Backup- und Recovery-Strategie bewegt sich in dem Spannungsverhältnis zwischen der Datenmenge und -Abhängigkeit, dem Infrastrukturaufbau und der Geschäftsform Ihrer Kunden. Auf Seiten des Gesetzes steht dem die eingangs erwähnte Verhältnismäßigkeit zwischen Aufwand und Risiko gegenüber.

Generell gilt, dass Sie Ihre Kunden in Sachen “Nachweisbare DSGVO-Konformität” umso besser unterstützen, je transparenter, nachvollziehbarer und granularer eine Lösung arbeitet. Um Ihre Kunden bestmöglich gegen unterschiedliche Szenarien abzusichern – und so die gesetzlich geforderte Sicherheit und Verfügbarkeit der Daten zu gewährleisten –, sind verschiedene, ineinandergreifende Ansatzpunkte zu beachten.

Führt man sich die unterschiedlichen Risiken vor Augen, denen Ihre Kundensysteme ausgesetzt sind – ob Naturkatastrophen, Hardware-Versagen, Cyberkriminalität oder menschliches Fehlverhalten –, wird schnell deutlich: Eine eindimensionale Sicherheitsstrategie reicht kaum aus. Vielmehr sollte ein Backup so aufgebaut sein, dass unterschiedliche Gefahrenquellen und Angriffspunkte abgedeckt werden. Eine einfache, aber bewährte Methode, um eine solche von Grund auf verlässliche Backup-Strategie zu entwickeln, ist die [3-2-1-Regel](#).⁶

Diese Regel zielt letztlich darauf ab, dass alle Backups auf demselben Stand redundant vorhanden sind. So ist das Risiko, dass alle Daten auf einen Schlag verloren gehen, auf ein verschwindendes Minimum reduziert, wenn

- **drei** Kopien aller kritischen Daten mindestens auf
- **zwei** unterschiedlichen Medien existieren, von denen
- **eines** offsite gelagert wird, d. h. an einem anderen Standort als die Original-Daten.

Wenn es um den datengetriebenen Geschäftsalltag Ihrer Kunden geht, gibt es zwei weitere Kriterien, die zu bedenken sind: Zum einen die Recovery Time Objective, also die Zeitspanne, über die ein Geschäftsprozess ausfallen kann, bis das Unternehmen Schaden nimmt. Und zum anderen die Recovery Point Objective, welche den Zeitraum beschreibt, der zwischen zwei Sicherungen liegen darf, bevor ein Datenverlust geschäftsschädigende Ausmaße annimmt.

Diese beiden Eckpunkte sollten ausschlaggebend sein, wenn es um den Backup-Zeitplan beziehungsweise den Umfang bei granularen Sicherungen geht. Nur so können Sie garantieren, dass Ihre Kunden auch im Ernstfall den Geschäftsbetrieb möglichst lückenlos wieder aufnehmen können.

Die Bedeutung der E-Mail-Archivierung

Obwohl es eine von mehreren Möglichkeiten ist, um die Datenintegrität nach der DSGVO zu gewährleisten, ergibt sich die gesetzliche Pflicht zur E-Mail-Archivierung in erster Linie aus dem GoBD.

Während das übergeordnete Ziel des Backups die Wiederherstellung – und damit die garantierte Verfügbarkeit der Daten nach Artikel 32 DSGVO – ist, steht das E-Mail-Archiv vor einem anderen Hintergrund. Obwohl es eine von mehreren Möglichkeiten ist, um die Datenintegrität nach der DSGVO zu gewährleisten, ergibt sich die gesetzliche Pflicht zur E-Mail-Archivierung in erster Linie aus dem GoBD. ⁷

Die “Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff” verpflichtet Unternehmen zur manipulationssicheren Aufbewahrung elektronischer Geschäftsdokumente, -vereinbarungen und -aufzeichnungen. Dabei müssen die genannten Materialien nicht nur auffindbar, sondern auch stets abrufbar sein. Ohne eine professionelle E-Mail-Archivierung kann ein Unternehmen diesen Anforderungen kaum vollumfänglich nachkommen.

Die GoBD betonen ferner die Wichtigkeit der Datensicherheit: Um Datensätze vor Verlust und unberechtigten Veränderungen zu schützen, sollte die E-Mail-Archivierung in das IT-Sicherheitskonzept und Krisenmanagement eingebunden werden. Wie beim Backup gilt auch hier: Die Erfüllung dieser Pflicht bietet Ihren Kunden nicht nur Rechtssicherheit, sondern auch zahlreiche weitere Vorteile im täglichen Geschäftsbetrieb – von der garantierten Auffindbarkeit von Nachrichten über eine verschlankte IT-Infrastruktur bis hin zu vereinfachten Administrationsprozessen. In Sachen Rechtssicherheit können Sie Ihre Kunden damit noch weiter unterstützen, indem Sie neben der DSGVO auch die Anforderungen der GoBD thematisieren und eine passende Strategie zur professionellen E-Mail-Archivierung anbringen.

4. Die Umsetzung: Lösungen für Sie als IT-Profi

Obwohl der Artikel 32 keinen konkreten Maßnahmen-Katalog liefert, lassen sich doch einige Rahmenkriterien ableiten, die bei der Wahl der geeigneten Backup- oder E-Mail-Archivierungslösung in Erwägung gezogen werden sollten.

Um Ihnen Übersicht und Zuordnung zu erleichtern, haben wir die wichtigsten Aussagen dieses Artikels sowie weitere technisch anwendbare Gesetzesabschnitte für Sie aufbereitet und mit einem Stichwort zur möglichen Umsetzung versehen:

Um ein angemessenes Sicherheitsniveau zu gewährleisten, sollte die Möglichkeit bestehen, personenbezogene Daten zu verschlüsseln. (Art. 32, Abs. 1 lit. a) DSGVO)

Verschlüsselung der Backup-Daten/des E-Mail-Archivs

Es müssen Maßnahmen getroffen werden, um die Vertraulichkeit und Integrität der Daten zu gewährleisten. (Art. 32 Abs. 1 lit. b) DSGVO)

Zuverlässiges Datenmanagement

Um die Verfügbarkeit der personenbezogenen Daten zu gewährleisten, müssen diese nach einem technischen oder physischen Zwischenfall schnellstmöglich wiederhergestellt werden. (Art. 32 Abs. 1 lit. c) DSGVO)

Datenverfügbarkeit und -wiederherstellung

Datenschutzverletzungen müssen innerhalb von 72 Stunden nach Bekanntwerden der Verletzung den Behörden gemeldet werden. (Art. 33 Abs. 1 DSGVO) ⁸

Meldepflicht

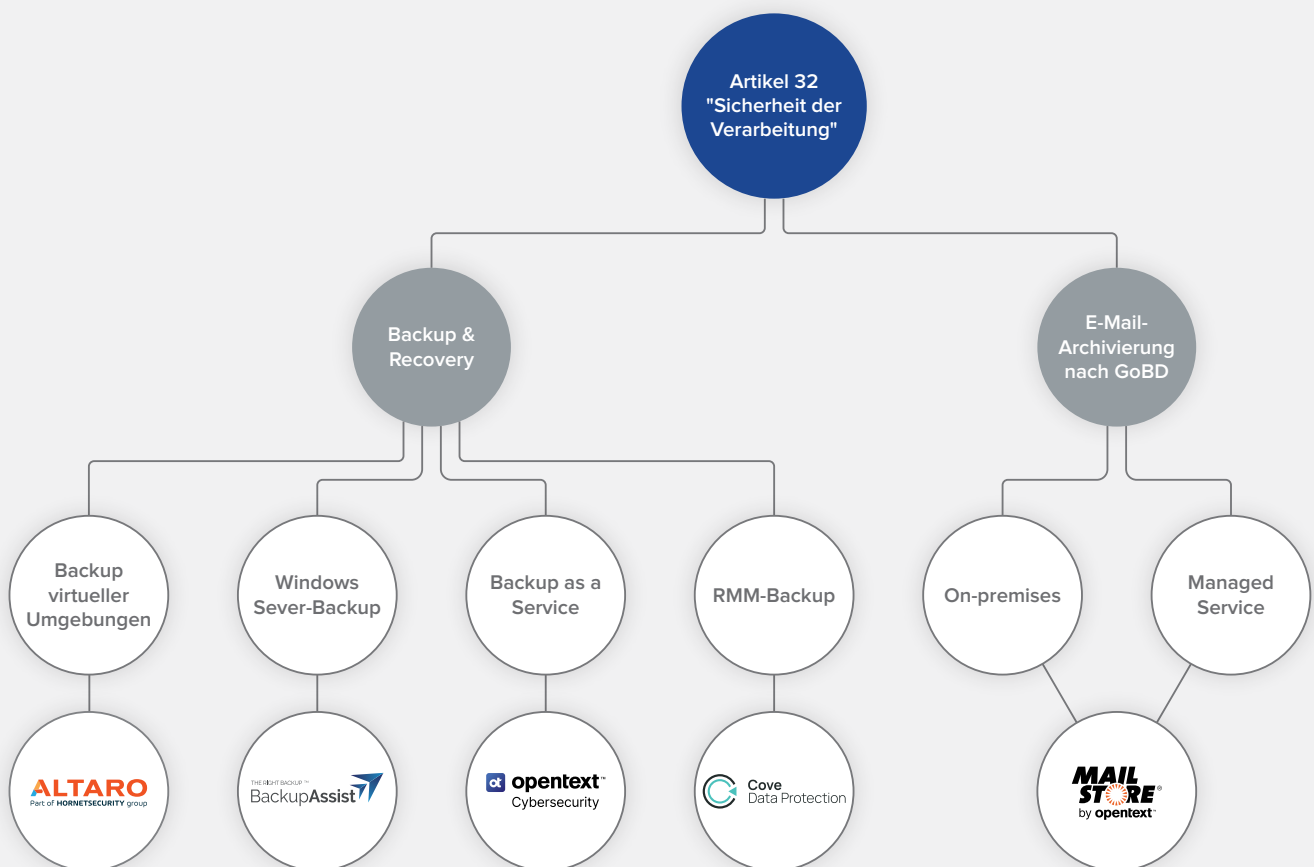
Den Aufbewahrungsfristen gegenüber steht das Recht auf Löschung, welches den Verantwortlichen unter bestimmten Umständen verpflichtet, die erhobenen Daten zu löschen. (Art. 17 DSGVO) ⁹

Aufbewahrungsfristen

Elektronische Geschäftsdokumente, -vereinbarungen und -aufzeichnungen müssen vollständig, manipulationssicher und jederzeit verfügbar aufbewahrt werden. (GoBD)

E-Mail-Archivierung

Bei der Frage nach der Umsetzung gilt es nun, nicht nur die technischen Rahmenbedingungen und Systemanforderungen bei Ihren Kunden zu bedenken, sondern auch die Struktur Ihres Service-Portfolios. Als IT-Profi ist es dabei natürlich Ihr Ziel, Ihren Kunden auch im Arbeitsalltag Mehrwerte zu bieten, welche über die schlichte Erfüllung der gesetzlichen Vorgaben hinaus gehen – sowohl in Sachen Backup und Recovery als auch bei der E-Mail-Archivierung. Aus diesem Grund finden Sie im folgenden Abschnitt des Whitepapers eine Lösungs-Übersicht zum Thema Backup und E-Mail-Archivierung.



4.1 Altaro – VM Backup für Hyper-V und VMware

[Altaro VM Backup](#) ist die weltweit führende Backup-Lösung zur Sicherung virtueller Maschinen unter Hyper-V und VMware. Die beste Inline-Deduplizierung der Branche – gepaart mit intuitiver Bedienung und alltagsnahen Features – bietet höchste Effizienz für Ihre Kunden. Gleichzeitig profitieren Sie als IT-Profi von der flexiblen Lizenzierung pro Host sowie der Wahlmöglichkeit zwischen der MSP- und der On-Premises-Variante.

Wie erfüllt Altaro die DSGVO?

Datenverfügbarkeit und -wiederherstellung

- Dank der Boot-from-Backup-Funktion können VMs sekundenschnell wieder in Betrieb genommen oder auf einem anderen Host wiederhergestellt werden.
- Granulare Wiederherstellung einzelner Dateien, Ordner oder Laufwerke ist möglich, ebenso die Wiederherstellung von Exchange-Servern bis auf E-Mail-Ebene.
- Backups von Live-VMs über die Nutzung des Microsoft VSS-Dienstes verhindert Ausfallzeiten.

Zuverlässiges Datenmanagement

- Intuitive Bedienung und einfache Administration erlauben das schnelle Aufsetzen von krisensicheren, automatisch verfolgten Backup-Plänen.
- Offsite-Sicherungen auf unterschiedlichsten Backup-Medien bieten maximale Flexibilität.
- Aufbewahrungsrichtlinien lassen sich für einzelne VMs individuell festlegen.

Verschlüsselung der Backup-Daten

- Altaro bietet AES-256-Verschlüsselung.
- Offsite-Sicherungen werden automatisch verschlüsselt.
- Editionsabhängig können Daten während des Backup-Prozesses einmalig mit einem Verschlüsselungscode versehen werden.

Meldepflicht

- Monitoring- und Reporting-Funktionen garantieren, dass der verantwortliche Administrator stets auf dem neuesten Stand ist und über korruptierte Backups informiert wird.

4.2 BackupAssist – führend bei Windows-Server-Backup

[BackupAssist](#) aus dem Hause Cortex I.T. gehört zu den weltweit führenden Backup-Lösungen für Windows-Server-Systeme, die in Leistungsumfang und Preisgestaltung speziell zugeschnitten ist auf die Bedürfnisse des KMU-Sektors. Die Anwendung ermöglicht vollautomatisch geplante Backups von Windows-Servern und Desktop-Systemen auf die unterschiedlichsten Backup-Medien – wie interne und externe Festplatten, NAS, iSCSI-Targets, RDX-Medien, Einzelbandlaufwerke und unterschiedliche Cloud-Speicherplätze. Die Möglichkeit zur zentralen Administration über den BackupAssist MultiSite Manager bietet Ihnen dabei eine enorme Zeitersparnis bei der Betreuung Ihrer BackupAssist-Installationen.

Wie erfüllt BackupAssist die DSGVO?

Datenverfügbarkeit und -wiederherstellung

- Ausgefallene oder beschädigte VMs können Sie mit Rapid VM Recovery sekundenschnell wieder in Betrieb nehmen.
- Einzelne Dateien, Ordner oder ganze Laufwerke lassen sich schnell und unkompliziert wiederherstellen.
- Backup-Pläne werden automatisch verfolgt.
- Bootfähige Backups (bestehend aus Boot-Laufwerk und Backup-Medium) machen Notfallwiederherstellung so einfach wie das Anschließen einer USB-Festplatte.

Zuverlässiges Datenmanagement

- Der CryptoSafeGuard schützt vor Ransomware, Viren und unbefugtem Zugriff.

Verschlüsselung der Backup-Daten

- BackupAssist bietet AES-256-Verschlüsselung, sowohl für bereits abgelegte Daten als auch für Datenströme während des Sicherungsprozesses.
- Verschlüsselte Container verhindern den Zugriff von Drittanbietern auf Cloud-Backups.
- Datensicherungen auf externen Wechselmedien wie USB-Festplatten oder RDX-Laufwerken lassen sich via BitLocker verschlüsseln.

Meldepflicht

- Der CryptoSafeGuard benachrichtigt bei einem Ransomware-Vorfall automatisch den Administrator via SMS und E-Mail.

4.3 OpenText Cybersecurity – Backup as a Service

[OpenText Cybersecurity](#) bietet Backup as a Service-Lösungen für Managed Services Provider: Unkompliziert und problemlos sichern Sie selbst komplexeste Systeme remote, plattformübergreifend und bandbreiteneffizient – dank patentierter DELTAPRO™-Technologie auf Ihrer eigenen Infrastruktur. Ob in der Private Cloud, onsite oder in einer hybriden Kombination: Die Backup-Strategien all Ihrer Kunden administrieren Sie über die multimandantenfähige, zentrale Verwaltungskonsole. Dabei stehen Ihnen mit einer Lizenz alle Anwendungsmöglichkeiten offen, während die Paketierung und Preisgestaltung an Ihre Kunden völlig Ihnen überlassen bleibt.

Wie erfüllt OpenText Cybersecurity die DSGVO?

Datenverfügbarkeit und -wiederherstellung

- Die granulare Herstellung einzelner Daten, Ordner oder ganzer Laufwerke ist problemlos möglich, bis hinunter zu E-Mails auf Exchange-Ebene.
- Einzelne Datensicherungen können versioniert werden, so dass auch ältere Datensätze entsprechend der Vorgaben zu Aufbewahrungspflichten wiederhergestellt werden können.
- Die OpenText-Lösungen sichern auch komplexe Umgebungen wie Microsoft Cluster Services, Linux oder Sun Solaris problemlos.
- Über die Einsatzdauer der Lösungen hinaus kann auf alte Backups zugegriffen werden.

Zuverlässiges Datenmanagement

- Mit OpenText Cybersecurity bieten Sie eine komplexe Backup-Strategie - inklusive automatisierter Offsite-Sicherung - entweder in der Private Cloud, onsite oder in einer hybriden Kombination.
- Passwort-Mechanismen und redundante Backup-Standorte schützen vor einer Datenmanipulation von innen.

Verschlüsselung der Backup-Daten

- Die OpenText-Lösungen verschlüsseln sowohl den Übertragungsweg der Daten als auch das vor Ort liegende Backup mittels AES-256-Verschlüsselung.
- Es können externe Verschlüsselungslösungen eingebunden werden.
- Die Lösungen folgen Industriestandards, einschließlich SOC 2, HIPAA, FERPA und GLBA.

Meldepflicht

- Monitoring- und Reporting-Optionen garantieren, dass der Verantwortliche über Vorgänge und eventuelle Fehler während des Backup-Prozesses informiert ist.



4.4 Cove Data Protection – Backup & Recovery

Die Hybrid-Cloud-Backup-Lösung [Cove Data Protection](#) lässt sich entweder vollständig in N-able N-sight RMM integrieren oder als Standalone-Variante betreiben. Cove Data Protection ist die einfache und zuverlässige hybride Cloud-Backup-Lösung zur Sicherung von Servern und Workstations für Microsoft Windows, Apple OS X- und Linux-Systeme. Zudem erlaubt Cove Data Protection die Sicherung von Microsoft Exchange-, SQL- und SharePoint-Servern sowie kompletter virtueller Maschinen wie Hyper-V oder VMware. Die Daten Ihrer Kunden liegen geschützt in einem deutschen Hochsicherheits-Rechenzentrum oder in Ihrem eigenen Rechenzentrum.

Wie erfüllt Cove Data Protection die DSGVO?

Datenverfügbarkeit und -wiederherstellung

- Einzelne Dateien bis hin zu kompletten SQL- oder Exchange-Datenbanken können unkompliziert wiederhergestellt werden.
- True Delta-Technologie erlaubt die rapide Sicherung von 9.000 Dateien pro Stunde.
- Kurze Backup-Zeitfenster garantieren Aktualität der Datensätze.

Zuverlässiges Datenmanagement

- Backups können wahlweise in der Cloud, in einem deutschen Hochsicherheits-Rechenzentrum oder im eigenen RZ gesichert werden.
- Lokale Sicherungen können auf NAS-Geräten angelegt werden.

Verschlüsselung der Backup-Daten/E-Mail-Archive

- Backups können mit AES 128-Bit, AES 256-Bit oder per 228-Bit-Blowfish- Verschlüsselung nach Militärstandard abgesichert werden.

Meldepflicht

- Die zentrale Verwaltung der Backups und Recovery-Statistiken über die webbasierte Management-Konsole garantiert Ihnen den bestmöglichen Überblick.



4.5 MailStore – rechtsichere E-Mail-Archivierung

Mit [MailStore](#) – ob unter MailStore Server, der MailStore Service Provider Edition oder MailStore Cloud – bieten Sie Ihren Kunden rechtskonforme, manipulationssichere E-Mail-Archivierung für jedes aktuelle Windows-Betriebssystem. Dabei stehen alle Archivierungs- und Verwaltungsfunktionen über den zentralen, responsiven Web Access zur Verfügung. Gemeinsam mit der intuitiven Bedienung und zeitsparenden Such- und Wiederherstellungsfunktionen erhöht sich so die Produktivität Ihrer Kunden noch weiter.

Wie arbeitet MailStore im Rahmen der DSGVO?

E-Mail-Archivierung

- MailStore bietet rechtskonforme, manipulationssichere E-Mail-Archivierung nach dem GoBD.
- Ein lokales E-Mail-Archiv ermöglicht das schnelle Wiederauffinden einzelner Nachrichten.
- Die intuitive Bedienung erlaubt Mitarbeitern das problemlose Auffinden und Wiederherstellen einzelner Nachrichten.

Zuverlässiges Datenmanagement

- Das lokale Archiv garantiert die Auskunftsfähigkeit und lässt sich zusätzlich in den Backup-Plan integrieren.

Verschlüsselung des E-Mail-Archivs

- MailStore verwendet SHA-Hashes und wendet auf E-Mail-Texte und Dateianhänge eine AES256-Verschlüsselung an.

Aufbewahrungsfristen

- Die Funktionen für das Lösch- und Aufbewahrungsmanagement von MailStore Server ermöglichen, beide Anforderungen zu erfüllen.

5. Das Backup & die DSGVO: Was sind Ihre nächsten Schritte?

Ein krisensicherer Backup- und Recovery-Plan ist für Ihre Kunden in Zukunft auch gesetzlich unverzichtbar. Hauptaugenmerk sollte dabei auf der Verfügbarkeit der Daten auch im Ernstfall liegen – das gilt auch für E-Mails, die geschäftskritische Absprachen enthalten.

Definieren Sie also schon jetzt den Handlungsbedarf bei Ihren Kunden und bieten Sie dank unseres breit gefächerten Portfolios individuell zugeschnittene Rechts- und Unternehmenssicherheit.

Selbstverständlich stehen wir Ihnen bei Fragen rund um unsere Backup- und Archivierungslösungen gern zur Verfügung – lassen Sie uns einfach wissen, wie wir Sie unterstützen können und kontaktieren Sie uns.

Quellenangaben

1. Art. 4 Abs. 1 DSGVO, [dsgvo-gesetz.de/art-4-dsgvo/](https://www.dsgvo-gesetz.de/art-4-dsgvo/)
2. Art. 1 Abs. 1 DSGVO, [dsgvo-gesetz.de/art-2-dsgvo/](https://www.dsgvo-gesetz.de/art-2-dsgvo/)
3. Art. 3 DSGVO, [dsgvo-gesetz.de/art-3-dsgvo/](https://www.dsgvo-gesetz.de/art-3-dsgvo/)
4. Art. 5 Abs. 3 DSGVO, [dsgvo-gesetz.de/art-83-dsgvo/](https://www.dsgvo-gesetz.de/art-83-dsgvo/)
5. [dsgvo-gesetz.de/art-32-dsgvo/](https://www.dsgvo-gesetz.de/art-32-dsgvo/)
6. www.elovade.com/blog/3-2-1-die-regel-fuer-ihr-erfolgreiches-backup/
7. www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuertemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.html
8. [dsgvo-gesetz.de/art-33-dsgvo/](https://www.dsgvo-gesetz.de/art-33-dsgvo/)
9. [dsgvo-gesetz.de/art-17-dsgvo/](https://www.dsgvo-gesetz.de/art-17-dsgvo/)

Rechtlicher Hinweis

Dieses Dokument dient lediglich der Information und stellt keine Rechtsberatung dar. Im konkreten Einzelfall wenden Sie sich bitte an einen spezialisierten Rechtsanwalt oder einen Datenschutzbeauftragten. Eine Gewähr und Haftung für die Richtigkeit aller Angaben wird nicht übernommen.

ELOVADE ▲

Kontakt Daten für Deutschland & Österreich:

ELOVADE Deutschland GmbH

sales@elovade.com

DE: +49 6441 67118 0

AT: +43 820 0010 36

elovade.com

Kontakt Daten für die Schweiz:

ELOVADE Swiss AG

sales@elovade.ch

CH: +41 55 552 27 00

elovade.ch