

Datenschutz-Grundverordnung (DSGVO) konforme Datenverwaltung

Christophe Bertrand, VP of Product Marketing

In der Vergangenheit wurden Personenbezogene Daten wie Name, Adresse, Telefonnummer, Geburtsdatum, Geschlecht, Alter und ethnische Zugehörigkeit mit Einwilligung der Individuen, durch das Ausfüllen von Formularen, Urlaubsbuchungen, Kauf von Eintrittskarten und Teilnahme an Verlosungen erfasst. Mit dem Fortschritt von sozialen Medien, Smartphones und Cloud Applikationen können Personenbezogene Daten jedoch auf weit indirekteren Wegen erfasst werden. Unsere IP Adresse und Standort können zum Beispiel von unserem Smartphone erfasst werden während wir in einem Café sitzen.

Allzu oft haben Einzelpersonen sehr wenig bis zu gar kein Einblick in welchem Maß und Umfang in dem ihre Daten erfasst, analysiert und geteilt werden. Letztendlich hat diese explosive Kombination aus schier unendlicher Datenerfassung und einer rasant ansteigenden Zahl der Vorfälle von Datenverlust zu einer neuen robusten Regulierung zum Schutz von Personenbezogene Daten geführt.

Mit dem schnellen Fortschritt technologischer Möglichkeiten und den grenzenlosen Möglichkeiten unserer modernen digitalen Wirtschaft mussten sich Regierungen anpassen um die Grundrechte ihrer Datensubjekte zu verbessern und ihnen einen besseren Datenschutz zu gewähren. Am 25. Mai 2018 wird die weltweit umfassendste Regulierung zum Datenschutz, die EU Datenschutz Grundverordnung (DSGVO), zum Gesetz.

Die DSGVO gibt den Bürgern der EU das Recht bei Unternehmen jedwede Daten die von ihnen gespeichert werden einzufordern, ihre Einwilligung zur Nutzung dieser Daten zurückzuziehen und ihre Vernichtung zu verlangen. Laut Artikel 12 der DSGVO muss dieses Verfahren einfach und kostenfrei sein und ohne Verzögerung spätestens im Zeitraum eines Monats vollzogen sein.

Das Ziel dieser Regulierung ist es die 28 EU Mitgliedsstaaten zu vereinheitlichen und Unternehmen zu mehr Verantwortung und Transparenz in Bezug auf die Daten die sie speichern anzuregen. Unabhängig von seinem Standort wird jegliches Unternehmen das Daten von EU Bürgern speichert oder verarbeitet dazu angehalten sein dies nach den Regeln dieses neuen Gesetzes zu tun. Es gibt den EU Bürgern Kontrolle über die Daten die ein Unternehmen von ihnen speichert.

Die EU hat den betroffenen Unternehmen und Organisationen ein Frist bis Mai 2018 gegeben, da die Implementierung der von der DSGVO vorgegebenen Prozesse und Kosten zeitaufwändig sein können. Angesichts des Umfangs und der transformierenden Reichweite der DSGVO ist es wichtig das Unternehmen und Organisationen analysieren wie sie mit persönlichen Daten umgehen.



Nichteinhaltung wird mit Strafen bis zu 4% vom weltweiten Umsatz oder Zwanzig Millionen Euro geahndet, was immer der höhere Betrag ist. In der Tat hat sich die Sachlage gedreht. Anstatt die Zahlung von Strafen wegen Nichteinhaltung vorzuziehen müssen Unternehmen und Organisationen jetzt in die Einhaltung der Anforderungen der DSGVO investieren um erhebliche Strafen zu vermeiden.

Die DSGVO erfordert eine umfangreiche Umgestaltung und rasche Maßnahmen in folgenden Bereichen:

- Rechenschaft und Verwaltung – Führung von Dokumentationsunterlagen zu Aktivitäten der Datenverarbeitung und Implementierung von Maßnahmen wie Prüfungen die die Konformität darlegen.
- Befristete Aufbewahrung - Persönliche Daten dürfen nicht länger aufbewahrt werden als für den ursprünglichen Grund der Erfassung notwendig.
- Verstoß Meldungen - Ein zu meldender Verstoß muss der entsprechenden aufsichtführenden Autorität binnen 72 Stunden nach der Feststellung von Seiten des Unternehmens mitgeteilt werden.
- Individuelle Rechte – Eine Einzelperson kann die Löschung oder Beseitigung von persönliche Daten anfordern, wenn es keinen zwingenden Grund für ihre Aufbewahrung gibt.

Unter diesen Bereichen weist Arcserve spezifisch auf die Notwendigkeit der Datensicherheit und der Vorbeugung von Datenverlusten hin. IT Umgebungen sollten höchstmoderne Technologien wirksam einsetzen um den Verlust von Daten vorzubeugen.

Heutzutage gibt es nicht eine einheitliche oder spezifische Lösung die sämtliche Vorgaben der DSGVO erfasst. Viele verschiedene Facetten wirken auf die IT und datenbezogene Prozesse wie Datensicherung und Archivierung ein.

Implikationen für Datensicherung und Archivierung

Artikel 5 der DSGVO legt die Grundprinzipien der Datensicherheit aus und beschreibt wie Unternehmen und Organisationen persönliche Daten verarbeiten und wie diese aufbewahrt und geschützt werden sollten. Artikel 5 legt dar das Unternehmen und Organisationen Sicherungen und Archivkopien von Daten aufbewahren dürfen solange diese auf eine Art und Weise verwaltet werden die die Sicherheit von persönlichen Daten gewährleistet.

Laut Artikel 5 der DSGVO müssen Personenbezogene Daten:

- (a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
- (b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke sollte nicht unvereinbar mit den ursprünglichen Zwecken sein;



- (c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein;
- (d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
- (e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke verarbeitet werden;
- (f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Die DSGVO inkludiert Maßnahmen die Rechenschaft und Verwaltung fördern. Diese ergänzen die Anforderungen zum Datenschutz der DSGVO. Das neue Rechenschaftsprinzip in Artikel 5(2) verlangt von Unternehmen einen Nachweis dafür zu erbringen, dass sie die Anforderungen erfüllen und legt explizit fest das dies ihre Pflicht ist.

- (a) Implementierung von technischen und organisatorischen Maßnahmen um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.
- (b) Führung von Dokumentationsunterlagen zu Aktivitäten der Datenverarbeitung.
- (c) Bestellung eines Datenschutzbeauftragten falls angemessen.
- (d) Implementierung von Maßnahmen zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.
- (e) Durchführung einer Datenschutz-Folgenabschätzung wo angemessen.

Arcserve erfüllt auf einzigartige Weise die Anforderungen der DSGVO

Die DSGVO erfordert eine verbesserte Datenverwaltung bei Datensicherung und Archivierung. Altlösungen für Datensicherung und Archivierung sind auf individuelle Herausforderungen bei der Datenverwaltung orientiert, deswegen stellen sie keine umfassende Option dar um den Anforderungen der DSGVO zu entsprechen. Arcserve hat einen einzigartigen Ansatz um mit einer robusten Produktpalette den breitgefächerten Anforderungen der DSGVO zu entsprechen.



Es ist ein weitgreifender Prozess erforderlich um festzulegen was in ihrem Unternehmen Personenbezogene Daten sind und wo sie sich befinden. Selbstverständlich sind Bereiche wie Datenbanken, Emails und PCs. Personenbezogene Daten ist ein breitgefächertes Begriff um Daten wie die persönliche E-Mail-Adresse, E-Mail-Adressen anderer und weitere Daten zu inkludieren die Unternehmen nicht nur für Marketing Aktivitäten, sondern auch als Bestandteil der Datensicherung und des Datenschutzes sammeln. Die DSGVO erfordert die Einwilligung des Eigners der Daten im Moment der Erfassung. Im Wesentlichen enthalten Datensicherungen und E-Mails Personenbezogene Daten die eine Bürde darstellen: Sämtliche Kopien der Datensicherung und archivierte E-Mails müssen nach DSGVO Anforderungen verwaltet werden.

Wenn eine Organisation Kopien der Datensicherung die Information von Europäischen Staatsbürgern enthält aufbewahrt, müssen sich diese Kopien in der EU befinden. Die Datensicherungen auf Festplattenspeicher, Band oder in der Cloud müssen in der EU residieren, es sei denn Sie verfügen über ein System in dem der Eigner der Daten Bewilligt das dies außerhalb der EU geschieht.

Unternehmen die E-Mail Archive unterhalten müssen die Anforderungen der DSGVO genau beachten. Es ist üblich das E-Mail Archive Daten wegen geschäftlichen, behördlichen oder rechtlichen Anforderungen über Jahre aufbewahren. In dem Fall das ein Nutzer seine Einwilligung zurückzieht ist es erforderlich das einem Administrator die Standardfunktionen der Lösung zur E-Mailarchivierung zu Verfügung stehen um die entsprechenden E-Mails zu identifizieren und sie zu löschen. Tätigkeitsprotokolle sind erforderlich um im Falle einer Prüfung den Beweis der Löschung erbringen zu können.

Unabhängig vom Hersteller ist es mit den heutzutage verwendeten Technologien zur Datensicherung nicht möglich Personenbezogene Daten aus der Datensicherung zu löschen.

- Dies würde ein massives Betrugsrisiko darstellen, wenn ein Individuum aus allen aktuellen und gesicherten Registern gelöscht werden könnte
- Es würde auch mit der Erfüllung von Anforderungen die eine Aufbewahrung und/oder Unveränderbarkeit von Daten erfordern in Konflikt stehen

Es ist erlaubt Personenbezogene Daten in der Datensicherung aufzubewahren, sogar wenn das Individuum sein Recht vergessen zu werden geltend gemacht hat. JEDOCH... ist es nicht erlaubt diese Daten wiederherzustellen (abgesehen davon, dass es einen rechtlichen Grund dafür gibt, wie zum Beispiele einen Rechtsprozess).

- Per DSGVO Erfüllung werden in Datensicherungen enthaltene Personenbezogene Daten als verfügt gekennzeichnet und dürfen nicht wiederhergestellt werden wenn das Individuum seine Einwilligung zurückgezogen hat.
- Wenn Sie eine Datensicherung die Personenbezogene Daten enthält die vergessen werden sollten wiederherstellen müssten, müssten Sie diese wieder löschen.
- Es besteht der Konsens, dass das Recht vergessen zu werden sich auf Live/Produktionsdaten vs. Archiv und Datensicherungen bezieht



Daten im allgemeinen, einschließlich Backup müssen geschützt werden (wie zum Beispiel Verschlüsselung). Arcserve's Produkte und Lösungen können dies bieten.

Wenn Sie Daten speichern die als personenbezogen oder empfindlich eingestuft werden können, wie zum Beispiel Kundendaten, dann müssen diese Daten (die Datensicherungen) an einem physischen Ort in der EU residieren.

Zum jetzigen Zeitpunkt kann gesagt werden das die DSGVO sowohl für Hersteller wie auch für Unternehmen diverse Grauzonen darstellt. Interpretierungen und Präzedenzfälle werden bei der Implementierung von Hilfe sein.

Arcserve Unified Data Protection (UDP)

Arcserve stellt Ressourcen zur Datensicherung auf Enterprise Niveau zur Verfügung, ohne die Komplexität die üblicherweise mit Enterprise-Lösungen zur Datensicherung in Verbindung gebracht wird. Kleine und überstrapazierte IT Teams können auf einfache Art und Weise Daten aus physikalischen, virtuellen und Cloud Umgebungen von und zu jedmöglicher Quelle und Ziel sichern, während Sie sämtliche Datensicherungsbezogene Aspekte aus einer einzigen, einfach eleganten Konsole einstellen und verwalten. Sobald sich die geschäftlichen Bedürfnisse oder Anforderungen ändern kann das IT Team einfach hoch performante Kapazitäten aktivieren ohne das beschwerliche Upgrades oder das Aufsetzen von zusätzlichen Lösungen erforderlich sind.

Eine Schlüsselanforderung der DSGVO wie in Artikel 5(2) gestellt ist das „der Kontrolleur ist verantwortlich und sollte im Stande sein die Einhaltung der Anforderung beweisen zu können“.

In Bezug auf die Erfüllung sind regelmäßige Datensicherungen, Wiederherstellungstests und Reports zu gesicherten Daten ein guter Weg um dem Datenschutzbeauftragten (neue Rolle) zu belegen das Sie die Anforderung erfüllen und effektiv Ihre Daten sichern und schützen.

Arcserve UDP kann hierbei unterstützen:

- Standard Reports belegen welche Datensicherungen am Laufen sind, welche Daten gesichert werden und wo/was das Ziel der Sicherung ist.
- Retention Reports belegen wie lange Kopien der Datensicherung aufbewahrt und wann sie zerstört werden.
- SLA und Assured Recovery Reports belegen die Sicherheit der Daten, inklusive Häufigkeit der Datensicherung und Dauer einer Wiederherstellung.



UDP Vorteile



Verbesserte Datensicherung, Wiederherstellung und Verfügbarkeit

- Eine einheitliche Lösung die Kern-Technologien zur Datensicherung unter einer Konsole vereint.
- Eine Lösung mit einem großen Spektrum an Funktionen die eine Vielfalt von Umgebungen unterstützt.
- Anpassbare Pläne zur Datensicherung um Kundenspezifischen Anforderungen zu entsprechen.
- Erweiterte Berichterstattung zum Beleg der Erfüllung der DSGVO Anforderungen.



Verbesserte Operative Effizienz

- Verbesserte Effizienz des Administrators durch Arcserve's einheitliche Verwaltungskonsole.
- Einfache Handhabung und großes Spektrum an Einsatzmöglichkeiten führen zu verbessertem time to value.
- Verringerte Netzwerk und Storage Belastung.



Verbesserte Funktionen um die Erfüllung der DSGVO Kriterien darzulegen

- Verschlüsselung schützt die Kopien der Datensicherung und entsprechend die Daten nach DSGVO vorgaben.
- Flexible Wiederherstellungsoptionen ermöglichen eine Verwaltung der Datensicherungen nach DSGVO Vorgaben.
- Vorbehaltungsoptionen unterstützen eine langfristige und gesetzliche Aufbewahrung so wie rechtlich unbedenkliche Content-Entsorgung.
- Optionen zum testen, messen und reporten von Wiederherstellungsprozessen zur Einhaltung der DSGVO vorgaben.

Arcserve UDP Archivierung

Arcserve UDP Archivierung ermöglicht es Unternehmen auf einfache Art und Weise Anforderungen bei der E-Mail suche, Konformität und rechtlichen Risiken mit einer spezifisch entwickelten Lösung vor Ort, in der privaten und in der öffentlichen Cloud zu erfüllen. Kleine und überstrapazierte IT Teams können ihre operative Effizienz verbessern und durch die Verwaltung sämtlicher Anforderungen der Datensicherung und E-Mail Archivierung aus einer einzigen, einfach eleganten Konsole kosten reduzieren.

Als neue Lösung in Arcserve UDP stellt die Technologie zur E-Mail Archivierung sämtliche Funktionen bereit um die Archivierung von E-Mails DSGVO konform zu gestalten. Sie unterstützt eine mandantenfähige Architektur und ermöglicht daher multinationalen und dezentralisierten Unternehmen die Suche nach E-Mails per Standort, Bereich oder Abteilung. So Kann zum Beispiel eine in einem Land der EU generierte E-Mail getrennt von in den Vereinigten Staaten generierten E-Mails verwaltet und archiviert werden.



Arcserve UDP Archivierung ist eine speziell entwickelte Lösung zur regulierungskonformen E-Mail Archivierung und stellt diverse Funktionen bereit um schnell auf DSGVO Anforderungen zum Recht vergessen zu werden reagieren zu können.

Für den Fall das ein Individuum seine Einwilligung zurückzieht verfügen Administratoren über integrierte eDiscovery Optionen um rasch nach allen empfangenen und versandten E-Mails des Individuums zu suchen, identifizieren und sie zu löschen. Administratoren haben Zugriff auf detaillierte Archivierungsprotokolle die sämtliche Aktionen belegen und als Beweis der Löschung dienen. Es ist zu beachten das dies ohne in Konflikt mit Konformitätsanforderungen zu treten getan werden sollte. Die DSGVO ist diesbezüglich nicht unbedingt klar.

Vorteile der UDP Archivierung auf einen Blick



Verwaltung von Archivierung, in einer einheitlichen Konsole



Schnelles und leistungsfähiges Suchen

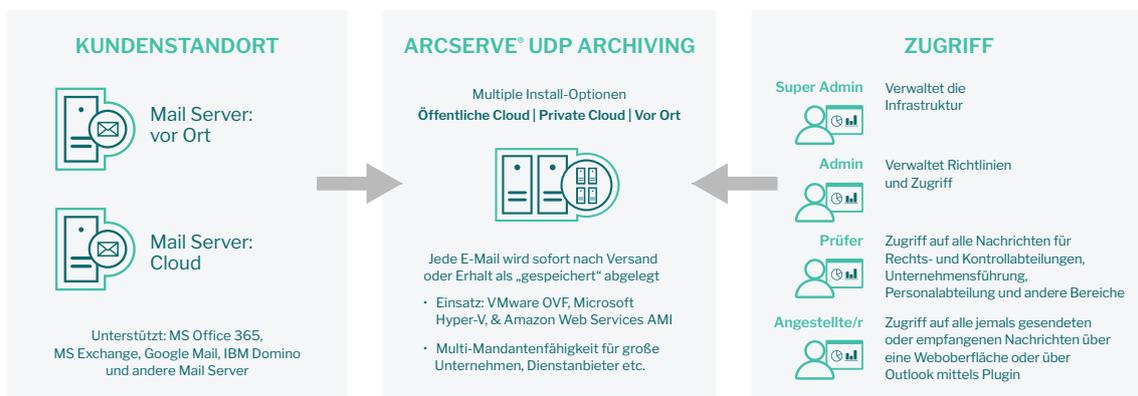


Mandantenfähige Archivierung, Suche und Verwaltung von E-Mails per Standort



Unbegrenzte Anzahl Postfächer per Suche.

Architektur der UDP Archivierung





Fazit

Die DSGVO gibt EU Bürgern das Recht ihre Einwilligung zurückzuziehen und die Zerstörung ihrer E-Mails und anderen personenbezogenen Daten zu verlangen. Dies führt zu einem neuen Szenario in dem Unternehmen und Organisationen neue Anforderungen einhalten müssen. Während viel über das Recht zur Löschung von personenbezogenen Daten gesprochen wird, handelt es sich hierbei nur um einen Aspekt der neuen Verordnung. Sie bezieht sich ganz klar auch auf den Schutz personenbezogener Daten, der seinerseits mit operativen Entscheidungen bei der Datensicherung und Wiederherstellung zusammenhängt.

Die für die Datensicherung und Verwaltung von E-Mails zuständigen Teams benötigen leistungsfähige und gleichzeitig einfach zu bedienende Lösungen die das rasche identifizieren und löschen von personenbezogener Daten in ihren Systemen ermöglicht. Arcserve UDP und seine Lösung zur E-Mail Archivierung stellen die notwendigen Ressourcen zu Verfügung um die Konformität mit den Anforderungen der DSGVO zu belegen, inklusive Datensicherung und Wiederherstellung aus einer einheitlichen Konsole, granulare Wiederherstellung mit der Möglichkeit spezifische Dateien auszuschließen und vollständige Aktivitätserfassung und Reporting um die Konformität zu belegen.

Sollte ein Individuum seine Einwilligung zurückzuziehen kann der Administrator anhand integrierter Funktionen umgehend persönliche E-Mails identifizieren und löschen, um so die Konformität mit Anforderungen der DSGVO zu garantieren und Sanktionen sowie Geldstrafen zu vermeiden. Arcserve UDP und seine Lösung zur E-Mail Archivierung sind ein wichtiger Bestandteil einer nachgiebigen Strategie zur Einhaltung der DSGVO. Arcserve entwickelt derzeit zusätzliche Funktionen innerhalb seines Produkt-Portfolios, um die GDPR-Compliance weiter zu unterstützen. Bitte kontaktieren Sie unsere Teams für weitere Details zu unseren Lösungen.

Für weitere Informationen besuchen Sie arcserve.com