Dateiübertragung und die Datenschutz-Grundverordnung

EU-Datenschutz-Grundverordnung Artikel 32 (2):

„Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu ***personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.***“

Progress® | ipswitch®

Vorbereitung auf die EU-Datenschutz-Grundverordnung

Die EU-Datenschutz-Grundverordnung (DSGVO) wurde vom Europäischen Parlament und Rat angenommen und tritt am 25. Mai 2018 in Kraft. Die DSGVO legt für Datenschutz einen hohen Standard fest und findet für sämtliche Unternehmen Geltung, die die personenbezogenen Daten von EU-Bürgern verarbeiten beziehungsweise die Verarbeitung überwachen. Die Nichteinhaltung der DSGVO kann zu Strafen in Höhe von 20 Millionen Euro oder von vier Prozent des jährlichen Umsatzes führen, je nachdem, welche Summe höher ist.

Die DSGVO definiert zwei Arten von Unternehmen, deren Aktivitäten reguliert sind: Verantwortlicher und Auftragsverarbeitender. Ein Auftragsverarbeitender ist ein Unternehmen, das personenbezogene Daten von EU-Bürgern erfasst, verarbeitet, speichert oder überträgt. Ein Verantwortlicher ist ein Unternehmen, das die Aktivitäten von Auftragsverarbeitenden lenkt. Das weitet die Verantwortung vom ursprünglichen Datenerfasser (in diesem Fall der Verantwortliche) auf die tatsächliche Datenerfassung durch einen Outsourcer oder Geschäftspartner (der Auftragsverarbeitende) aus. Unter der DSGVO sind sowohl der Verantwortliche als auch der Auftragsverarbeitende für den Schutz der Daten verantwortlich und können bei Nichteinhaltung zu Strafzahlungen verpflichtet werden. In der Beziehung zwischen einem Verantwortlichen und einem Auftragsverarbeitenden ist die Koordinierung der Compliance-Bemühungen hinsichtlich der Übertragung von Daten angebracht. Egal in welcher der beiden Rollen sich Unternehmen wiederfinden, sie müssen dennoch die für den Datenschutz relevanten Kontrollen, Verfahren sowie die Technologie überprüfen (und wahrscheinlich verbessern). Bei diesem Vorhaben sollten alle Bemühungen auf Artikel 32 der DSGVO abgestimmt werden, der besagt, dass die implementierten Sicherheitsmaßnahmen auf das Risiko abgestimmt sind.

ARTIKEL 32 (1):

VERANTWORTLICHE UND AUFTRAGSVERARBEITENDE MÜSSEN „EIN DEM RISIKO ANGEMESSENES SCHUTZNIVEAU (...) GEWÄHRLEISTEN“

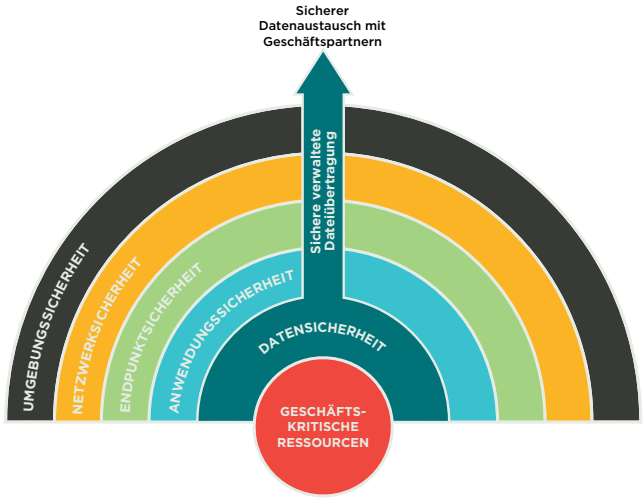
ARTIKEL 32 (1):

„(...) INSBESONDERE DIE RISIKEN [SIND] ZU BERÜCKSICHTIGEN,“ DIE MIT UNBEABSICHTIGTER VERNICHTUNG, VERLUST ODER VERÄNDERUNG, UNBEFUGTER OFFENLEGUNG VON BEZIEHUNGSWEISE UNBEFUGTEM ZUGANG ZU PERSONENBEZOGENEN DATEN, DIE ÜBERMITTELT, GESPEICHERT ODER AUF ANDERE WEISE VERARBEITET WURDEN – VERBUNDEN SIND.

Dateiübertragungen sind risikoreich

Die Wahrscheinlichkeit ist hoch, dass Ihr Unternehmen bereits umfassend in eine Sicherheitsinfrastruktur investiert hat. Im Rahmen der DSGVO muss der Wert berücksichtigt werden, den weitere Ausgaben in traditionellen Gebieten gegenüber Personalschulungen, neuen Verfahren und notwendigen Technologieinvestitionen bieten, die übersehen wurden.

Die externe Übertragung von personenbezogenen Daten ist heute über viele verschiedene Branchen hinweg ein zentraler Betriebsgeschäftsprozess von IT-



ARTIKEL 4 (2):

„VERARBEITUNG“ BEZEICHNET JEDEN AUSGEFÜHRTEN VORGANG WIE DAS ERHEBEN, DAS ERFASSEN, DIE ORGANISATION, DAS ORDNEN, DIE SPEICHERUNG, (...) ÜBERMITTLUNG, VERBREITUNG ODER EINE ANDERE FORM DER BEREITSTELLUNG

Unternehmen. Was die Sicherheit betrifft, sind Daten während der Übertragung gefährdet, da sie eine einmalige Gelegenheit zum Abfangen während der Übertragung, für unbefugten Zugriff beim Speichern zum Herunterladen auf einem Transfer-Server, der Zustellung an einen unbefugten Empfänger oder der falschen Handhabung bei Verarbeitung am Ziel darstellen.

Es ist ganz offensichtlich, dass externe Datenübertragungen von personenbezogenen Daten in der Vorbereitungsphase auf die DSGVO große Aufmerksamkeit erfordern. Unter dem Druck mit Zeitmangel und begrenzten Ressourcen umzugehen, sehen sich Unternehmen gezwungen, ihre Ausgaben für die Einhaltung der DSGVO auf die Verarbeitungsaktivitäten zu bündeln, die für sensible personenbezogene Daten das größte Risiko darstellen.

Die Datenübertragung wird aus gutem Grund in der DSGVO ausdrücklich als Verarbeitungsaktivität genannt. Datenübertragungsaktivitäten können personenbezogene Daten einem hohen Risiko aussetzen. Beispiel:

- In Dateien gespeicherte personenbezogene Daten, die auf einen FTP-Server hochgeladen werden, sind unverschlüsselt und werden selten gelöscht.
- Der Modus „Anonymous FTP“, veraltete Sicherheitspatches und sonstige Schwachstellen bieten Cyberkriminellen einfachen Zugriff.
- Desktop-Benutzer können IT-Vorrichtungen umgehen und personenbezogene Daten auf unsichere Art und Weise zum Beispiel per E-Mail oder über cloudbasierte File-Sharing-Dienste versenden.
- Durch Mangel zentraler Kontrollen über Berechtigungen werden die Anmeldeinformationen von Benutzern offengelegt, die Hacker nutzen können, um Kontrolle über geschützte Daten zu erlangen.
- Da keine zentralen und gesicherten Prüfprotokolle vorhanden sind, besteht das Risiko, dass unbefugte oder fehlgeschlagene Übertragungen unbemerkt bleiben.

Datenschutz-Grundsätze der DSGVO

In der DSGVO werden Datenschutz-Grundsätze aufgeführt, die Unternehmen einhalten müssen. Viele dieser Grundsätze beziehen sich auf die Übertragung personenbezogener Daten.

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	Rec 39, Artikel 5 (1) (a)	Zusätzliche Sorgfalt beim Erstellen und Umsetzen von Datenverarbeitungsaktivitäten
Datensicherheit	Rec 29, 71, 156 Artikel 5 (1) (f), 24 (1), 25 (1,2), 28, 29, 32	Sicherstellung, dass personenbezogene Daten vor unbefugter interner und externer Verarbeitung, unbeabsichtigtem Verlust, Zerstörung und Schädigung geschützt sind
Richtigkeit	Rec 39, Artikel 5 (1) (d)	Treffen aller angemessenen Maßnahmen, damit die Richtigkeit der personenbezogenen Daten sichergestellt werden kann
Rechenschaftspflicht	Rec 85, Artikel 5 (2)	Die Einhaltung der Datenschutz-Grundsätze muss nachgewiesen werden
Zweckbindung	Rec 50, Artikel 5 (1) (b)	Personenbezogene Daten, die für einen Zweck erhoben wurden, dürfen nicht für einen neuen unvereinbaren Zweck verwendet werden
Datenminimierung	Rec 39, Artikel 5 (1) (c)	Ausschließliche Verarbeitung personenbezogener Daten auf dem Zweck angemessene Weise
Speicherbegrenzung	Rec 39, Artikel 5 (1) (e)	Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist

Sichere FTP-Server sind nicht konform

Der Upgrade-Versuch einer bereits bestehenden FTP-Umgebung für Compliance mit der Datenschutz-Grundverordnung ist unzulänglich. Sie müssten sicherstellen, dass alle externen Übertragungsprozesse sichere Protokolle (SFTP, FTPS und HTTPS) und Verschlüsselung (SSH, TLS und SSL) nutzen. Außerdem müssten Sie allen Upload-Prozessen die AES-256-Verschlüsselung hinzufügen, damit Daten nach der Übertragung geschützt werden. Diese Optimierungen reichen allerdings nicht aus. Das sichere FTP bringt viele der Risiken und Schwachstellen der FTP-Server mit sich, die es ersetzt.

Wenn es in Ihrem Unternehmen eine „FTP-Ausbreitung“ gab, besteht möglicherweise ein Durcheinander verschiedener FTP-Server mit unterschiedlicher Software auf unterschiedlichen Plattformen mit unterschiedlichen Softwareversionen, Betriebssystemversionen und Sicherheitspatches. Dies schafft Schwachstellen, die Cyberkriminelle für den Zugriff auf personenbezogene Daten nutzen können.

	Sicheres FTP								Skripte			
	Protokolliert Daten während der Übertragung	Schützt Daten nach der Übertragung	Dateiintegritäts-prüfung	Nichtabstreit-barkeit	Content-Scanning	Gateway-Proxy-Server	Ad-hoc-Datei-übertragung	Sensitive Zugriffskontrolle	Gesicherte Prüfprotokolle	Aufgabenbasierte Dateiübertragung	Zentralisierte Kontrolle	Warnmeldungen in Echtzeit	Analysen
Datensicherheit	✓		✓									✓	
Grundsatz der Zweckbindung													
Datenminimierung													
Richtigkeit													
Speicherbegrenzung													
Rechenschaftspflicht	✓		✓										
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	✓		✓										

FTP-Datenübertragungen sind in der Regel abhängig von Skripten. Skripte können in verschiedenen Sprachen wie PERL, BASH, VB und PowerShell verfasst werden und sind häufig undokumentiert. Ohne Vereinheitlichung und zentrale Kontrolle können skriptbasierte Workflows, die auf mehreren FTP-Servern installiert sind, zur unbefugten Verarbeitung personenbezogener Daten führen.

Schließlich erfordert die Datenschutz-Grundverordnung von den IT- und Sicherheitsteams einen Compliance-Nachweis. Die Erfassung und das Reporting mit Prüfprotokollen von mehreren FTP-Servern ist zeitaufwändig und lässt bei den Prüfern, die eine einzige Quelle für Protokolldaten in einem konsistenten Format mit Speicherung in einer gesicherten Datenbank bevorzugen, die Alarmglocken läuten.

VERMEIDEN SIE EINE AUSBREITUNG VON FTP-SERVERN

- X UNVERSCHLÜSSELTE DATEIEN
- X KEINE ZENTRALISIERTEN PROTOKOLLDATEIEN
- X GEGEBENENFALLS UNDOKUMENTIERTE SKRIPTE
- X PRÜFER WERDEN MISSTRAUISCH

Diese Einschränkungen anzugehen ist sehr zeit- und kostenaufwändig, da Datenübertragungsumgebungen den Standards der Datenschutz-Grundverordnung angepasst werden müssen. Die Frage lautet: Was spricht dafür? Ein weiterer Aspekt ist, dass Prüfer im Rahmen der Datenschutz-Grundverordnung wenig Verständnis für ausgleichende Kontrollen zeigen.

Vorteile von MOVEit

Datenschutz-Grundsatz der DSGVO: Rechtmäßige, auf Treu und Glauben beruhende Verarbeitung, Datensicherheit und Richtigkeit

- √ MOVEit bietet Sicherheitsfunktionen zur Erfüllung bestimmter Anforderungen, die in den Artikeln 5, 24, 25, 28, 32 und 39 dargelegt sind. Dazu gehören:
- √ Verschlüsselung personenbezogener Daten während der Übertragung und nach dem Speichern
- √ Nichtabstreitbarkeit zur Validierung, dass personenbezogene Daten nur zwischen autorisierten Absendern und Empfängern übertragen werden
- √ Integration in Lösungen zur Verhinderung von Datenverlust und Virenschutzlösungen
- √ Browser- und Microsoft Outlook-Integration zur Sicherstellung, dass Desktop-Clients eine von der IT autorisierte Lösung für die sichere Datenübertragung verwenden
- √ Umgebungssicherheit, damit unverschlüsselte personenbezogene Daten nicht in die DMZ gelangen
- √ Zentrale, sensitive Zugriffskontrolle zum Schutz von Anmeldeinformationen, Berechtigungen und personenbezogenen Daten

Durch die Dateiintegritätsprüfung kann validiert werden, dass personenbezogene Daten nicht verändert wurden.

MOVEit schützt personenbezogene Daten während der Übertragung mithilfe sicherer Datenübertragungsprotokolle wie SFTP, FTPS und HTTPS sowie der Verschlüsselungsprotokolle SSH, TLS und SSL. MOVEit schützt Daten nach der Übertragung mithilfe der AES-256-Verschlüsselung.

Die MOVEit-Funktion zur Nichtabstreitbarkeit validiert, dass personenbezogene Daten nur zwischen autorisierten Absendern und Empfängern übertragen werden. Dies ist eine Schutzmaßnahme zur Verhinderung von Man-in-the-Middle-Angriffen, bei denen Daten während der Übertragung abgefangen oder manipuliert werden. Durch die automatische Dateiintegritätsprüfung wird validiert, dass eine Datei nicht verändert wurde – eine zusätzliche Schutzmaßnahme für den Richtigkeitsgrundsatz der Datenschutz-Grundverordnung.

Die Lösung bietet zusätzlichen Schutz durch Integration in Content-Scanning-Lösungen wie Datenverlust- und Virenschutzsoftware. Alle Content-Scanning-Aktivitäten werden protokolliert und bei Erkennung von Datenverlust oder Malware erfolgt eine Benachrichtigung.

Bei MOVEit Gateway handelt es sich um einen Proxy-Server, der sich in der DMZ befindet und sicherstellt, dass keine personenbezogenen Daten in der DMZ gespeichert werden. Alle eingehenden Verbindungen in der DMZ werden beendet und es wird sichergestellt, dass jegliche Kommunikationen an das vertrauenswürdige Netzwerk über einen sicheren Kanal erfolgen.

Die Ad-hoc-Funktion bietet eine Datenübertragung für Desktop-Clients, die leicht zu erlernen und zu verwenden ist. Benutzer können große Dateien sicher über einen Webbrowser oder Microsoft Outlook versenden. Dadurch wird das Risiko verringert, dass Benutzer vertrauliche Daten offenlegen, indem sie IT-Einrichtungen mit unsicheren cloudbasierten File-Sharing-Lösungen umgehen.

MOVEit verfügt über eine eigene integrierte sichere Datenbank, mit der Anmeldeinformationen von Benutzern und Berechtigungen geschützt werden. Aufgrund der einzigartigen Kombination aus verschlüsseltem Speicher und sicheren Berechtigungen ist MOVEit nicht auf die Sicherheit des zugrundeliegenden Betriebssystems angewiesen, in der Hacker bekannte Schwachstellen nutzen können.

Datenschutz-Grundsatz der DSGVO: Rechenschaftspflicht

Der Grundsatz der Rechenschaftspflicht verlangt von Unternehmen, dass sie Compliance mit den Datenschutz-Grundsätzen der DSGVO nachweisen. Unternehmen müssen Prüfpfade für alle Datenübertragungsaktivitäten, bei denen personenbezogene Daten im Spiel sind, erfassen und sichern. MOVEit verfolgt alle Dateiübertragungsaktivitäten einschließlich Authentifizierungen und Änderungen an Workflows in einer gesicherten Datenbank nach.

MOVEit führt automatische Erfassungen und Reporting mit Datenübertragungsprotokollen durch – an einem zentralen konsolidierten Ort. Die MOVEit-Prüfprotokolle sind gesichert und deren Richtigkeit ist vertrauenswürdig.

Datenschutz-Grundsätze der DSGVO: Zweckbindung, Datenminimierung und Speicherbegrenzung

Durch die Grundsätze Zweckbindung, Datenminimierung und Speicherbegrenzung wird die Verarbeitung personenbezogener Daten für einen bestimmten Zweck und zur ausschließlichen Bereitstellung der Daten beschränkt, die für diesen Zweck erforderlich sind und anschließend gelöscht werden müssen.

MOVEit ersetzt Skripte mit einer formularbasierten Lösung, die eine standardisierte, sicherere und dokumentierte Datenübertragung ermöglicht. MOVEit zentralisiert

die Kontrolle über alle Datenübertragungsaktivitäten. Dank der integrierten Planung können Unternehmen allgemeine, sich wiederholende Datenübertragungsaufgaben planen. Unternehmen können Aufgaben nach der Übertragung einschließen, zum Beispiel die geplante Löschung personenbezogener Datendateien. Umfangreiche Analysen liefern den erforderlichen Einblick in Übertragungsaktivitäten. So kann fortwährende Compliance mit den Datenschutz-Grundsätzen der DSGVO sichergestellt werden.

MOVEit und die Einhaltung der Datenschutz-Grundsätze der DSGVO

Die kostengünstige Option mit dem geringsten Risiko ist eine verwaltete Datenübertragungslösung wie Progress MOVEit. Bei MOVEit handelt es sich um eine zentralisierte und konsolidierte Datenübertragungslösung. Darin wird die sichere Datenübertragung in zentralisierte Workflows, Zugriffskontrolle und Prüfprotokollierung integriert. Die Lösung bietet vollständige hohe Verfügbarkeit und Failover. Das Ergebnis: Weniger bewegliche Einheiten, was ein geringeres Risiko für personenbezogene Daten bedeutet, und weniger Zeitaufwand und Kosten für die Verwaltung und Unterstützung von Verarbeitungsaktivitäten bei der Datenübertragung.

	MOVEit Transfer								MOVEit Automation				
	Protokolliert Daten während der Übertragung	Schützt Daten nach der Übertragung	Dateiintegritäts-prüfung	Nichtabstreit-barkeit	Content-Scanning	Gateway-Proxy-Server	Ad-hoc-Datei-übertragung	Sensitive Zugriffskontrolle	Gesicherte Prüfprotokolle	Aufgabenbasierte Dateiübertragung	Zentralisierte Kontrolle	Warnmeldungen in Echtzeit	Analysen
Datensicherheit	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Grundsatz der Zweckbindung									✓	✓	✓		✓
Datenminimierung									✓	✓	✓		✓
Richtigkeit			✓	✓	✓				✓				
Speicherbegrenzung									✓	✓	✓		✓
Rechenschaftspflicht	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓

Über Progress

Progress (NASDAQ: PRGS) bietet eine führende Plattform für die Entwicklung und Bereitstellung von strategischen Geschäftsanwendungen. Wir ermöglichen unseren Partnern die Bereitstellung moderner und überzeugender digitaler Erlebnisse mit einem Bruchteil an Aufwand, Zeit und Kosten. Progress bietet leistungsstarke Tools für das mühelose Erstellen anpassbarer Anwendererlebnisse unabhängig von Gerätetypen oder Touchpoint, die Flexibilität einer serverlosen Cloud-Lösung zur Entwicklung von modernen Anwendungen, führende Datenkonnektivitätstechnologie, Web Content Management, sicheren Datenaustausch, Netzwerk-Monitoring, sowie eine preisgekrönte Machine-Learning-Lösung, die die Integration kognitiver Funktionen in jeder beliebigen Anwendung ermöglicht. Über 1.700 unabhängige Software-Anbieter, 100.000 Unternehmenskunden sowie 2 Millionen Entwickler setzen bei der Ausführung Ihrer Anwendungen auf Progress. Weitere Informationen zu Progress erhalten Sie unter www.progress.com oder unter +1-800-477-6473.

Erfahren Sie, wie MOVEit Sie auf die DSGVO vorbereitet

Progress®
MOVEit®

Laden Sie Ihre KOSTENFREIE TESTVERSION unter MOVEit herunter!