Zusammenfassung Datenschutz-Grundverordnung

Artikel • 03.10.2021 • 10 Minuten Lesedauer • 2 Mitwirkende

In diesem Artikel

Begrifflichkeiten
Was ist die DSGVO?
Verwenden Sie den Microsoft Compliance Manager, um Ihr Risiko einzuschätzen
Antrag einer betroffenen Person
Datenschutzfolgenabschätzung
Benachrichtigung bei Sicherheitsverletzungen
Prüflisten zu Rechenschaftspflicht für die DSGVO
Häufig gestellte Fragen zur DSGVO
Weitere Ressourcen

Die Datenschutz-Grundverordnung (DSGVO) führt neue Regeln für Organisationen ein, die Waren und Dienstleistungen in der Europäischen Union (EU) anbieten oder Daten von in der EU ansässigen natürlichen Personen erfassen und analysieren, unabhängig von deren Wohnsitz und Unternehmenssitz. Dieses Dokument bietet Ihnen Informationen zu der Einhaltung von Rechten und dem Erfüllen von Verpflichtungen unter der DSGVO, während Sie Microsoft-Produkte und -Dienste verwenden. Ein empfohlener DSGVO-Aktionsplan und Prüflisten zu Rechenschaftspflicht bieten zusätzliche Ressourcen zum Bewerten und Implementieren der DSGVO-Compliance.

Begrifflichkeiten

Hilfreiche Definitionen für DSGVO-Ausdrücke, die in diesem Dokument verwendet werden:

- **Datenverantwortlicher (Verantwortlicher)**: eine juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
- **Personenbezogene Daten und betroffene Person**: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann.

- **Auftragsverarbeiter**: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
- **Kundendaten**: Daten, die im Rahmen Ihrer regulären Geschäftstätigkeit erstellt und gespeichert werden.

Was ist die DSGVO?

Die DSGVO gibt Personen die Berechtigung, personenbezogene Daten zu verwalten, die von einer Organisation erfasst werden. Diese Rechte können über einen Antrag einer betroffenen Person ausgeübt werden. Die Organisation muss rechtzeitig Informationen zu Anträgen betroffener Personen und zu Datenschutzverletzungen bereitstellen und Datenschutzfolgenabschätzungen durchführen.

Beim Implementieren oder Bewerten von DSGVO-Anforderungen sollten mehrere Punkte berücksichtigt werden:

- Entwickeln oder Auswerten Ihrer DSGVO-Datenschutzrichtlinie für Compliance-Daten.
- Bewerten der Datensicherheit in Ihrer Organisation.
- Wer ist Ihr Datenverantwortlicher?
- Welche Datensicherheitsabläufe müssen Sie möglicherweise ausführen?

Der empfohlene DSGVO-Aktionsplan und Prüflisten zu Rechenschaftspflicht können zusätzliche Punkte auf den Plan rufen, die es zu bedenken gilt.

Die folgenden Aufgaben sind erforderlich, um die DSGVO-Standards zu erfüllen. Folgen Sie den Links in der Liste, um Details zu Ihrer Implementierung zu erhalten.

- **Anträge betroffener Personen**. Ein von einer betroffenen Person formal gestellter Antrag an einen Verantwortlichen, bestimmte Maßnahmen (Änderung, Einschränkung, Zugriff) im Zusammenhang mit den personenbezogenen Daten der betroffenen Person zu ergreifen.
- **Benachrichtigung bei Sicherheitsverletzungen**. Unter der DSGVO besteht eine Verletzung personenbezogener Daten in „einem Sicherheitsverstoß, der zur zufälligen oder unrechtmäßigen Zerstörung, zu Verlust, Veränderung, unbefugter Weitergabe von oder unberechtigtem Zugang zu übermittelten, gespeicherten oder anderweitig verarbeiteten personenbezogenen Daten führt".
- **Datenschutzfolgenabschätzungen**. Datenverantwortliche sind unter der DSGVO dazu aufgerufen, eine Datenschutzfolgenabschätzung für Prozesse vorzubereiten, die „wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen".

Wie weiter oben erwähnt, bieten der empfohlene DSGVO-Aktionsplan und die Prüflisten zu Rechenschaftspflicht einen Leitfaden zur Implementierung oder Bewertung der Konformität von DSGVO bei der Verwendung von Microsoft-Produkten und -Diensten.

Verwenden Sie den Microsoft Compliance Manager, um Ihr Risiko einzuschätzen

Microsoft Compliance Manager ist eine Funktion im Microsoft 365 Compliance Center, die Ihnen hilft, die Compliance-Position Ihres Unternehmens zu verstehen und Maßnahmen zu ergreifen, um Risiken zu reduzieren. Der Compliance Manager verfügt über eine vorgefertigte Bewertung für diese Vorschrift für Enterprise E5-Kunden. Die Vorlage für die Erstellung der Bewertung finden Sie auf der Seite **Bewertungsvorlagen** im Compliance Manager. Erfahren Sie, wie Sie Bewertungen im Compliance Manager erstellen.

Antrag einer betroffenen Person

Die DSGVO gewährt Personen bestimmte Rechte in Verbindung mit der Verarbeitung ihrer personenbezogenen Daten, einschließlich des Rechts zur Korrektur falscher Daten, zum Löschen von Daten bzw. zur Einschränkung ihrer Verarbeitung, zum Empfangen von Daten und zum Erfüllen einer Anforderung zur Übertragung der Daten an einen anderen Controller. Der Verantwortliche ist für die Bereitstellung einer zeitgerechten, DSGVO-konsistenten Antwort verantwortlich. Technische Details finden Sie unter Anträge betroffener Personen.

Häufig gestellte Fragen (FAQs) zum Antrag einer betroffenen Person

Welche Aktionen sind zum Durchführen eines Antrags einer betroffenen Person erforderlich?

Anträge betroffener Personen umfassen sechs Aktivitäten: Erkennung, Zugang, Berichtigung, Einschränkung, Export und Löschung.

Was sind Ihre Datenquellen?

Ein großer Teil der Daten einer Organisation wird in Office-Anwendungen wie Excel und Outlook generiert. Möglicherweise finden Sie auch relevante Daten für einen Antrag einer betroffenen Person in den von Microsoft-Produkten und -Diensten generierten Erkenntnissen und vom System generierten Protokollen.

Welche Arten von Daten müssen durchsucht werden?

Personenbezogene Daten finden Sie in den Kundendaten, den von Microsoft-Produkten und -Diensten generierten Erkenntnissen sowie in vom System generierten Protokollen.

Wie werden personenbezogene Daten durchsucht?

Die Suche nach personenbezogenen Daten kann unter Microsoft-Produkten und -Diensten variieren. Suchtools bieten beispielsweise eine Inhaltssuche oder eine In-App-Suche. Administratoren können auf vom System generierte Protokolle zugreifen, die einer Benutzeraktivität zugeordnet sind.

In welchen Formaten sollten personenbezogene Daten zur Verfügung gestellt werden?

Das „Recht auf Datenübertragbarkeit" der DSGVO ermöglicht es betroffenen Personen, eine elektronische Kopie ihrer personenbezogenen Daten in einem „strukturierten, gängigen, maschinenlesbaren Format" sowie die Übermittelung dieser Dateien durch Ihre Organisation an einen anderen Datenverantwortlichen anzufordern.

Wie sehen die Anforderungen der DSGVO aus und was sind meine Verantwortlichkeiten als Controller?

Als Controller sind Sie gemäß der DSGVO zu Folgendem verpflichtet:

- Sie geben Datensubjekten eine Kopie ihrer personenbezogenen Daten sowie eine Erläuterung der Kategorien ihrer Daten, die verarbeitet werden. Sie benennen den Zweck dieser Verarbeitung ebenso wie die Kategorien von Drittanbietern, denen die Daten eventuell offengelegt werden.
- Sie unterstützen jeden einzelnen Nutzer dabei, sein Recht auszuüben, falsche personenbezogene Daten zu korrigieren, Daten zu löschen oder ihre Verarbeitung einzuschränken, seine eigenen Daten in lesbarer Form abzurufen und ggf. eine Anfrage zur Übertragung der Daten an einen anderen Controller zu stellen.

Wie sehen die Anforderungen der DSGVO aus und was sind die Microsoft-Verantwortlichkeiten als Verarbeiter?

Microsoft muss Ihnen die notwendigen technischen und organisatorischen Mittel an die Hand geben, damit Sie adäquat auf Anfragen von Datensubjekten reagieren können, die ihre oben beschriebenen Rechte in Anspruch nehmen.

Wo finde ich Informationen in Verbindung mit der DSGVO für lokale Server?

Eine Reihe von Artikeln zur DSGVO finden Sie hier. Sie wurden von Microsoft erstellt und bieten empfohlene Ansätze für die lokale Arbeitslast für SharePoint Server,

Exchange Server, Project Server, Office Web Apps Server, Office Online Server und lokale Dateifreigaben.

Welche Mittel gibt Microsoft Ihnen an die Hand, um auf Anfragen von Datensubjekten zu reagieren?

Online Services bietet ein breites Spektrum an Funktionalitäten, die Sie als Controller nutzen können, um auf Anfragen von Datensubjekten zu reagieren. Microsoft-Unternehmensonlinedienste und Administratorsteuerelemente unterstützen Sie dabei, auf personenbezogene Daten im Rahmen von Datenbetreffsanforderungen zu reagieren, sodass Sie personenbezogene Daten, die sich in den vom Controller verwalteten Daten befinden, die in der Cloud von Microsoft gespeichert sind, auffinden, korrigieren, einschränken, löschen, exportieren und darauf zugreifen können. Online Services stellt Daten bei Bedarf auch in maschinenlesbarer Form bereit.

Datenschutzfolgenabschätzung

Unter der DSGVO sind Datenverantwortliche dazu aufgerufen, eine Datenschutzfolgenabschätzung (Data Protection Impact Assessment, DPIA) für Prozesse vorzubereiten, die „wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen“. Microsoft-Produkte und -Dienste an sich machen keine Datenschutzfolgenabschätzung erforderlich. Vielmehr hängt dies von den Details Ihrer Microsoft-Konfiguration ab. Eine Liste der Details, die in Office berücksichtigt werden müssen, finden Sie in Inhalte einer Datenschutzfolgenabschätzung.

Häufig gestellte Fragen zur Datenschutzfolgenabschätzung

Wann sollten Sie eine Datenschutzfolgenabschätzung durchführen?

Verantwortliche sind dazu aufgefordert, eine Datenschutzfolgenabschätzung hinsichtlich Risiken für die Sicherheit personenbezogener Daten oder als Reaktion auf eine Datenschutzverletzung auszuführen. Spezifische Beispiele für Risikofaktoren in Office werden in Ist eine Datenschutzfolgenabschätzung notwendig? behandelt.

Was ist für die Durchführung einer Datenschutzfolgenabschätzung erforderlich?

Die DSGVO gibt vor, dass eine Datenschutzfolgenabschätzung Folgendes umfasst:

- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung in Bezug auf den Zweck der Datenschutzfolgenabschätzung.
- Eine Bewertung der Risiken für die Rechte und Freiheiten betroffener Personen.

- Vorgesehene Maßnahmen zum Umgang mit den Risiken, Sicherheitsvorkehrungen, Sicherheitsmaßnahmen und Mechanismen zur Sicherstellung des Schutzes personenbezogener Daten und zur Einhaltung der Compliance mit der DSGVO.

Was sind meine Verantwortlichkeiten als Controller?

Die DSGVO sieht vor, dass Sie als Datencontroller vor der Verarbeitung von Daten, die mit hoher Wahrscheinlichkeit ein großes Risiko für die Rechte und Freiheiten einzelner Personen darstellt, eine Datenschutz-Folgenabschätzung auszuführen. Dies gilt inbesondere dann, wenn bei der Datenverarbeitung neue Technologien eingesetzt werden. Im Folgenden finden Sie eine an die DSGVO angelehnte, nicht vollständige Liste von Fällen, in denen eine Datenschutz-Folgenabschätzung ausgeführt werden muss:

- Automatisierte Verarbeitung zum Zweck der Profilerstellung und für ähnliche Aktivitäten, die rechtliche Auswirkungen haben oder sich in ähnlicher Weise wesentlich auf betroffene Personen auswirken;
- Umfassende Verarbeitung spezieller Kategorien von personenbezogenen Daten, d. h. Daten, aus denen die ethnische Herkunft, die politische Gesinnung oder Ähnliches hervorgeht, bzw. Daten zu strafrechtlichen Verurteilungen und Straftaten;
- Systematische Überwachung eines öffentlich zugänglichen Bereichs.

Aus der DSGVO geht außerdem hervor, dass die Aufsichtsbehörde konsultiert werden muss, falls Datenverarbeitungsvorgänge ein hohes Risiko für betroffene Personen bergen, das Sie nicht durch geeignete Verfahren eindämmen können.

Was sind die Verantwortlichkeiten von Microsoft?

Microsoft bietet in seinen Engineering- und Business-Bereichen sowohl standardmäßige als auch speziell zugeschnittene Datenschutzoptionen an. Im Rahmen dieser Bemühungen führt Microsoft umfassende Überprüfungen des Datenschutz bei Verarbeitungsvorgängen durch, die sich möglicherweise auf die Rechte und Freiheiten von Personen auswirken können. Datenschutzteams, die in die Dienstgruppen eingebettet sind, überprüfen das Design und die Implementierung von Diensten, um sicherzustellen, dass personenbezogene Daten auf respektvolle Art verarbeitet werden, die im Einklang mit internationalen Gesetzen, Benutzererwartungen und unseren ausdrücklichen Verpflichtungen stehen.

Diese Datenschutzüberprüfungen sind in der Regel ausführlich – ein bestimmter Dienst wird möglicherweise dutzende oder hunderte Male überprüft. Microsoft fasst diese ausführlichen Datenschutzüberprüfungen in Bewertungen der Auswirkungen des Datenschutzes zusammen, die größere Verarbeitungsgruppierungen umfassen, die dann

vom Microsoft EU-Datenschutzbeauftragten überprüft werden. Der Datenschutzbeauftragte beurteilt die Risiken im Zusammenhang mit der Datenverarbeitung, um sicherzustellen, dass entsprechende Abhilfemaßnahmen vorhanden sind. Wenn der Datenschutzbeauftragte nicht abwendbare Risiken findet, werden Empfehlungen an die Engineering-Gruppe gegeben. Wenn sich Risiken im Zusammenhang mit dem Datenschutz ändern, werden die Bewertungen der Auswirkungen des Datenschutzes überprüft und aktualisiert.

In der Funktion des Datenverarbeiters ist Microsoft verpflichtet, Datencontroller dabei zu unterstützen, die in der DSGVO formulierten Anforderungen an Datenschutz-Folgenabschätzungen zu erfüllen. Zur Unterstützung unserer Kunden wurden die relevanten Abschnitte der DPIAs von Microsoft zusammengefasst und werden in diesem Abschnitt in künftigen Updates bereitgestellt, damit Controller die Microsoft-Dienste nutzen können, um die Zusammenfassungen für die Erstellung eigener DPIAs zu verwenden.

Benachrichtigung bei Sicherheitsverletzungen

Die DSGVO sieht für die Verletzung des Schutzes personenbezogener Daten eine Informationspficht für Datencontroller und Datenverarbeiter vor. Als Datenauftragsverarbeiter stellt Microsoft sicher, dass unsere Kunden die DSGVO-Anforderungen zur Benachrichtigung bei Sicherheitsverletzungen erfüllen. Die Datenverantwortlichen sind dafür verantwortlich, die Datenschutzrisiken zu bewerten und zu beurteilen, ob ein Kunde über eine Datenschutzverletzung benachrichtigt werden muss. Microsoft stellt die Informationen zur Verfügung, die für diese Einschätzung erforderlich sind. Weitere Informationen darüber, wie Microsoft eine Verletzung des Schutzes personenbezogener Daten erkennt und darauf reagiert, finden Sie in Benachrichtigung bei Datenschutzverletzungen im Rahmen der DSGVO.

Häufig gestellte Fragen zu Benachrichtigung bei Sicherheitsverletzungen

Was stellt eine Verletzung personenbezogener Daten im Rahmen der DSGVO dar?

Personenbezogene Daten beziehen sich auf alle Informationen im Zusammenhang mit einer Person, die verwendet werden können, um diese Person direkt oder indirekt zu identifizieren. Eine Verletzung personenbezogener Daten stellt „einen Sicherheitsverstoß dar, der zur zufälligen oder unrechtmäßigen Zerstörung, zu Verlust, Veränderung, unbefugter Weitergabe oder unberechtigtem Zugang zu übermittelten, gespeicherten oder anderweitig verarbeiteten personenbezogenen Daten führt“.

Was sind Ihre Verantwortlichkeiten als Controller?

Wenn eine Verletzung personenbezogener Daten, die möglicherweise die Rechte und Freiheiten von Personen gefährdet (z. B. Diskriminierung, Identitätsdiebstahl, Betrug, finanzielle Schäden oder Schädigung ihres Rufs) auftritt, sind Sie im Rahmen der DSGVO zu Folgendem verpflichtet:

- Benachrichtigen Sie die entsprechende Datenschutzbehörde innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls – beispielsweise, nachdem Sie von Microsoft benachrichtigt wurden. Wenn Sie die Datenschutzbehörde innerhalb dieses Zeitraums nicht benachrichtigen, müssen Sie hierzu eine Erklärung abliefern. Diese Erklärung an die Datenschutzbehörde ist auch dann erforderlich, wenn das Risiko für Personen nicht hoch ist.
- Benachrichtigen Sie die betroffenen Personen unverzüglich über die Verletzung.
- Dokumentieren Sie den Verstoß, einschließlich einer Beschreibung der Art der Verletzung – z. B. wie viele Personen betroffen waren, die Anzahl betroffener Datensätze, die Auswirkungen der Verletzung sowie alle Abhilfemaßnahmen, die Ihre Organisation vorschlägt oder ergriffen hat.

Was sind die Verantwortlichkeiten von Microsoft als Verarbeiter?

Nachdem Microsoft auf eine Verletzung des Schutzes personenbezogener Daten aufmerksam gemacht wurde, sind wir im Rahmen der DSGVO dazu verpflichtet, Sie unverzüglich darüber zu informieren. Hat Microsoft die Rolle des Datenverarbeiters inne, spiegeln unsere Pflichten sowohl DSGVO-Anforderungen als auch unsere konzerneigenen, weltweiten Standardvertragsbestimmungen wider. In unseren Augen gilt dies für alle bestätigten Verletzungen des Schutzes personenbezogener Daten und unabhängig von dem potenziellen Schadensrisiko. Wir informieren unsere Kunden darüber, ob die Verletzung des Schutzes personenbezogener Daten bei Microsoft selbst oder bei einem unserer Unterauftragsverarbeiter auftrat. Wir haben Prozesse implementiert, mit denen wir die Verantwortlichen bei Sicherheitsvorfällen in Ihrer Organisation schnell identifizieren und kontaktieren können. Darüber hinaus sind alle Unterauftragsverarbeiter vertraglich verpflichtet, Verletzungen der Sicherheit personenbezogener Daten in ihren eigenen Systemen an Microsoft zu melden und dahingehende Garantien zu geben.

Wie erkennt Microsoft eine Datenschutzverletzung?

Alle unsere Dienste und Mitarbeiter befolgen interne Incident-Management-Prozeduren, um sicherzustellen, dass alle Vorsichtsmaßnahmen zur Vermeidung von Verletzungen der Schutzes personenbezogener Daten ergriffen werden. Darüber hinaus hat Online Services spezifische plattformübergreifende Sicherheitskontrollen zur frühzeitigen Erkennung solcher Verletzungen implementiert.

Wie reagiert Microsoft auf eine Verletzung des Schutzes personenbezogener Daten?

Für die Verletzung des Schutzes personenbezogener Daten bietet Microsoft Ihnen folgende Unterstützung: - Entsprechend geschultes Sicherheitspersonal, das die zu befolgenden Prozeduren kennt. - Richtlinien, Verfahren und Steuerungselemente, um sicherzustellen, dass Microsoft detailliert Aufzeichnung führt. In der Reaktion gehört die Dokumentation des Sachverhalts eines Vorfalls, seiner Auswirkungen und der ergriffenen Abhilfemaßnahmen ebenso wie das Nachverfolgen und Speichern der Informationen in unseren Incident-Management-Systemen.

Wie informiert Microsoft mich über eine Verletzung des Schutzes personenbezogener Daten?

Microsoft hat Richtlinien und Prozeduren implementiert, um Sie umgehend zu benachrichtigen. Damit Sie Ihrer Informationspflicht gegenüber der Datenschutzbehörde nachkommen können, stellen wir eine Beschreibung des Prozesses bereit, der befolgt wurde, um zu ermitteln, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, ebenso wie eine Beschreibung der Art der Verletzung sowie der ergriffenen Gegenmaßnahmen.

Prüflisten zu Rechenschaftspflicht für die DSGVO

Diese Prüflisten ermöglichen einen bequemen Zugriff auf Informationen, die Sie bei der Einhaltung der DSGVO bei Verwendung von Microsoft-Produkten benötigen. Sie können Checklistenelemente mit Microsoft Compliance Manager verwalten, indem Sie unter „Vom Kunden verwaltete Steuerelemente“ in der GDPR-Kachel auf die Kontroll-ID und den Kontrolltitel verweisen.

Häufig gestellte Fragen zur DSGVO

Hat Microsoft Verpflichtungen gegenüber seinen Kunden bezüglich der DSGVO?

Ja. Die DSGVO sieht vor, dass Verantwortliche (z. B. Unternehmen, die Microsoft Enterprise Online Services nutzen) nur mit Auftragsverarbeitern (z. B. Microsoft) zusammenarbeiten, die ausreichende Sicherheiten für die Einhaltung der zentralen DSGVO-Anforderungen bieten. Microsoft setzt sich proaktiv dafür ein, diesen Verpflichtung gegenüber allen Volumenlizenzkunden im Rahmen ihrer Verträge nachzukommen.

Wie hilft mir Microsoft bei der Compliance?

Microsoft bietet Tools und Dokumentationen zur Unterstützung Ihrer DSGVO-Verantwortlichkeit. Dazu gehören die Unterstützung der Rechte der Betroffenen, die Durchführung eigener Datenschutz-Folgenabschätzung und die Zusammenarbeit bei der Aufklärung von Verletzung des Schutzes personenbezogener Daten.

Welche Verpflichtungen stehen in den DSGVO-Bedingungen?

Die DSGVO-Bedingungen von Microsoft stellen die in Artikel 28 erforderlichen Verpflichtungen für Verarbeiter dar. Artikel 28 setzt voraus, dass die Verarbeiter folgende Aufgaben ausführen:

- Verwenden von Subverarbeitern nur mit Zustimmung des Verantwortlichen, und für die Subverarbeiter haften.
- Verarbeiten von personenbezogenen Daten nur nach Anweisung des Verantwortlichen, auch im Hinblick auf Übertragungen.
- Sicherstellen, dass Personen, die personenbezogene Daten verarbeiten, zur Vertraulichkeit verpflichtet sind.
- Implementieren von geeigneten technischen und organisatorischen Maßnahmen, um ein Maß an Sicherheit bei den personenbezogenen Daten zu gewährleisten, die für das Risiko angemessen sind.
- Unterstützen der Verantwortlichen bei ihren Verpflichtungen zur Beantwortung der Anforderungen der betroffenen Person, ihre DSGVO-Rechte wahrzunehmen.
- Einhaltung der Vorschriften zur Meldung und Unterstützung bei Verletzung des Schutzes personenbezogener Daten.
- Unterstützen der Verantwortlichen mit der Datenschutz-Folgenabschätzung und der Beratung mit den Aufsichtsbehörden.
- Löschen oder Zurückgeben von personenbezogenen Daten am Ende der Erbringung von Diensten.
- Unterstützen des Verantwortlichen nachweislich der Einhaltung der DSGVO.

Auf welcher Grundlage erleichtert Microsoft die Übertragung von personenbezogenen Daten in Länder außerhalb der EU?

Microsoft verwendet seit langem die Standardvertragsklauseln (auch als Modellklauseln bekannt) als Grundlage für die Datenübertragung für seine Unternehmens-Online-Dienste. Die Standardvertragsklauseln sind von der Europäischen Kommission zur Verfügung gestellte Standardbedingungen, die verwendet werden können, um Daten konform außerhalb des Europäischen Wirtschaftsraums zu übertragen. Microsoft hat die Standardvertragsklauseln über die Bedingungen für Online-Dienste in alle unsere Volumenlizenzverträge aufgenommen. Für personenbezogene Daten aus dem Europäischen Wirtschaftsraum, der Schweiz und dem Vereinigten Königreich stellt Microsoft sicher, dass die Übermittlung personenbezogener Daten in ein Drittland oder

an eine internationale Organisation den entsprechenden Bestimmungen gemäß Artikel 46 der DSGVO unterliegt. Zusätzlich zu Microsofts Verpflichtungen unter den Standardvertragsklauseln für Auftragsverarbeiter und anderen Musterverträgen hält sich Microsoft weiterhin an die Bedingungen des EU-US-Datenschutzschild-Frameworks , wird sich aber nicht mehr darauf als Grundlage für die Übermittlung personenbezogener Daten aus der EU/dem EWR in die Vereinigten Staaten stützen.

Was sind die anderen Microsoft Compliance-Angebote?

Als globales Unternehmen mit Kunden in fast allen Ländern der Welt verfügt Microsoft über ein robustes Compliance-Portfolio zur Unterstützung unserer Kunden. Eine vollständige Liste unserer Compliance-Angebote einschließlich FedRamp, HIPAA/HITECH, ISO 27001, ISO 27002, ISO 27018, NIST 800-171, UK G-Cloud und viele andere finden Sie unter unseren Themen für Compliance-Angebote.

Wie wirkt sich die DSGVO auf mein Unternehmen aus?

Die DSGVO erlegt Unternehmen, die persönliche Daten erfassen und verarbeiten, zahlreiche Anforderungen auf, einschließlich einer Verpflichtung zur Einhaltung von sechs Schlüsselprinzipien:

- *Transparenz*, *Fairness* und *Rechtmäßigkeit* in der Handhabung und Nutzung personenbezogener Daten. Sie müssen sich gegenüber Einzelpersonen darüber im Klaren sein, wie Sie personenbezogene Daten verwenden, und benötigen außerdem eine „gesetzliche Grundlage" für die Verarbeitung dieser Daten.
- Beschränkung der Verarbeitung personenbezogener Daten auf *festgelegte*, *ausdrückliche* und *rechtmäßige Zwecke*. Sie sind nicht in der Lage, personenbezogene Daten für Zwecke wiederzuverwenden oder weiterzugeben, die mit dem Zweck, für den die Daten ursprünglich gesammelt wurden, nicht „kompatibel" sind.
- *Die Minimierung der Sammlung und Speicherung von personenbezogenen Daten* auf das Maß, das für den beabsichtigten Zweck angemessen und relevant ist.
- Gewährleistung der *Richtigkeit der personenbezogenen Daten* und Ermöglichung ihrer *Löschung oder Berichtigung*. Sie müssen Maßnahmen ergreifen, um sicherzustellen, dass die in Ihrem Besitz befindlichen persönlichen Daten korrekt sind und bei Fehlern korrigiert werden können.
- *Begrenzen der Speicherung von personenbezogenen Daten*. Sie müssen sicherstellen, dass Sie personenbezogene Daten nur so lange aufbewahren, wie es für die Erreichung der Zwecke, für die Daten gesammelt wurden, erforderlich ist.
- Gewährleistung von *Sicherheit*, *Integrität* und *Vertraulichkeit personenbezogener Daten*. Ihre Organisation muss Maßnahmen ergreifen, um personenbezogene Daten durch technische und organisatorische Sicherheitsmaßnahmen zu schützen.

Sie müssen die spezifischen Verpflichtungen Ihres Unternehmens gemäß DSGVO kennen und wissen, wie Sie diese einhalten. Microsoft unterstützt Sie auf Ihrem Weg zur DSGVO.

Welche Rechte müssen Unternehmen laut der DSGVO gewähren?

Die DSGVO gibt den in der EU ansässigen Personen die Kontrolle über ihre personenbezogenen Daten durch eine Reihe von „Rechten der betroffenen Personen". Dazu gehört das Recht auf:

- Zugriff zu Informationen darüber, wie personenbezogene Daten verwendet werden.
- Zugriff zu personenbezogenen Daten im Besitz einer Organisation.
- Die Löschung oder Berichtigung unrichtiger personenbezogener Daten zu veranlassen.
- Personenbezogene Daten unter bestimmten Umständen berichtigen und löschen lassen (manchmal auch als „Recht auf Vergessenwerden" bezeichnet).
- Beschränken oder Einspruch gegen die automatisierte Verarbeitung personenbezogener Daten erheben.
- Erhalten einer Kopie der personenbezogenen Daten.

Was sind Auftragsverarbeiter und Verantwortliche?

Ein Verantwortlicher ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Ein Verarbeiter ist eine natürliche oder juristische Person, öffentliche Behörde, Agentur oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Gilt die DSGVO für Verarbeiter und Verantwortlicher?

Ja, die DSGVO gilt sowohl für Verantwortliche als auch für Verarbeiter. Die Verantwortlichen müssen nur Verarbeiter einsetzen, die Maßnahmen ergreifen, um die Anforderungen der DSGVO zu erfüllen. Nach der DSGVO sind Verarbeiter im Vergleich zur Datenschutzrichtlinie mit zusätzlichen Pflichten und Haftung für die Nichteinhaltung oder das Handeln außerhalb der vom Verantwortlichen erteilten Anweisungen konfrontiert. Zu den Aufgaben des Verarbeiters gehören unter anderem, ohne darauf beschränkt zu sein:

- Verarbeitung von Daten nur auf Anweisung des Verantwortlichen.
- Verwendung geeigneter technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten.
- Unterstützung des Verantwortlichen bei Anfragen der betroffenen Person.

- Dadurch wird sichergestellt, dass die von ihr eingesetzten Subverarbeiter diese Anforderungen erfüllen.

Wie hoch können die Strafen bei Nichteinhaltung sein?

Unternehmen können bei Nichterfüllung bestimmter DSGVO-Anforderungen mit einer Geldbuße von bis zu € 20 Mio. oder 4 % des weltweiten Jahresumsatzes belegt werden, je nachdem, welcher Betrag höher ist. Zusätzliche individuelle Abhilfemaßnahmen könnten Ihr Risiko erhöhen, wenn Sie sich nicht an die DSGVO-Anforderungen halten.

Muss mein Unternehmen einen Datenschutzbeauftragten (Data Protection Officer, DPO) ernennen?

Sie hängt von mehreren Faktoren ab, die in der Verordnung genannt werden. Artikel 37 der DSGVO besagt, dass die Verantwortliche und die Verarbeiter in jedem Fall einen Datenschutzbeauftragten benennen müssen: a) die Verarbeitung durch eine Behörde oder Einrichtung der öffentlichen Hand erfolgt, mit Ausnahme von Gerichten in ihrer gerichtlichen Eigenschaft; b) die Kerntätigkeiten des Verantwortlichen oder des Verarbeiters bestehen, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zweckbestimmung eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Maßstab erfordern; oder c) die Kerntätigkeiten des Verantwortlichen oder des Verarbeiters besonderer Datenkategorien gemäß Artikel 9 und personenbezogener Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten nach Artikel 10 in großem Maßstab bestehen.

Wie hoch sind die Kosten für die Einhaltung der DSGVO?

Die Einhaltung der DSGVO wird für die meisten Unternehmen Zeit und Geld kosten, obwohl es für diejenigen, die in einem gut durchdachten Cloud-Service-Modell arbeiten und über ein effektives Data-Governance-Programm verfügen, ein reibungsloserer Übergang sein kann.

Wie kann ich feststellen, ob die Daten, die meine Organisation verarbeitet, unter die DSGVO fallen?

Die DSGVO regelt die Erfassung, Speicherung, Verwendung und Weitergabe „personenbezogener Daten“. Personenbezogene Daten werden in der DSGVO allgemein als alle Daten definiert, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Zu den personenbezogenen Daten können unter anderem Online-Identifikatoren (z. B. IP-Adressen), Mitarbeiterinformationen, Vertriebsdatenbanken, Daten des Kundendienstes, Kundenfeedback-Formulare, Standortdaten, biometrische Daten, CCTV-Aufnahmen, Aufzeichnungen über Treueprogramme, Gesundheits- und

Finanzinformationen und vieles mehr gehören. Diese können sogar Informationen enthalten, die nicht personenbezogen zu sein scheinen – wie beispielsweise ein Foto einer Landschaft ohne Menschen – wenn diese Informationen durch eine Kontonummer oder einen eindeutigen Code mit einer identifizierbaren Person in Verbindung stehen. Und selbst personenbezogene Daten, die pseudonymisiert wurden, können personenbezogene Daten sein, wenn das Pseudonym mit einer bestimmten Person in Verbindung gebracht werden kann.

Die Verarbeitung bestimmter „spezieller" Kategorien personenbezogener Daten – wie z. B. personenbezogene Daten, welche die ethnische Herkunft einer Person offenbaren oder ihre Gesundheit oder sexuelle Ausrichtung betreffen – unterliegt strengeren Regeln als die Verarbeitung „gewöhnlicher" personenbezogener Daten. Diese Auswertung der personenbezogenen Daten ist sehr faktenspezifisch, weshalb wir empfehlen, einen Experten zu beauftragen, um Ihre spezifischen Umstände zu beurteilen.

Meine Organisation verarbeitet nur Daten im Auftrag anderer. Muss sie noch die DSGVO einhalten?

Ja. Obwohl sich die Regeln etwas unterscheiden, gilt die DSGVO sowohl für Organisationen, die Daten für eigene Zwecke sammeln und verarbeiten („Verantwortliche"), als auch für Organisationen, die Daten im Auftrag anderer verarbeiten („Verarbeiter"). Diese Anforderung stellt eine Abkehr von der bestehenden Datenschutzrichtlinie dar, die für Verantwortlichen gilt.

Was gilt insbesondere als personenbezogenen Daten?

Personenbezogene Daten sind alle Informationen, die eine identifizierte oder identifizierbare Person betreffen. Es wird nicht zwischen privaten, öffentlichen oder beruflichen Rollen einer Person unterschieden. Zu den persönlichen Daten gehören:

- Name
- Private Adresse
- Geschäftliche Adresse
- Telefonnummer
- Mobiltelefonnummer
- E-Mail-Adresse
- Reisepassnummer
- Personalausweisnummer
- Sozialversicherungsnummer (oder ähnlich)
- Führerschein
- Physische, physiologische oder genetische Informationen
- Medizinische Informationen

- Kulturelle Identität
- Bankdetails/Kontonummern
- Steuernummer
- Geschäftliche Adresse
- Kreditkartennummer/EC-Kartennummer
- Beiträge für soziale Medien
- IP-Adresse (EU-Raum)
- Standort-/GPS-Daten
- Cookies

Kann ich Daten außerhalb der EU übertragen?

Ja, aber die DSGVO regelt streng die Übertragung von personenbezogenen Daten europäischer Bürger an Orte außerhalb des Europäischen Wirtschaftsraums. Möglicherweise müssen Sie einen bestimmten rechtlichen Mechanismus, wie z. B. einen Vertrag, einrichten oder sich an einen Zertifizierungsmechanismus halten, um diese Übertragungen zu ermöglichen. Microsoft erläutert die von uns verwendeten Mechanismen in den Bedingungen für Online-Dienste.

Ich habe Anforderungen an die Datenaufbewahrung durch Compliance. Haben diese Anforderungen Vorrang vor dem Recht auf Löschung?

Wenn es berechtigte Gründe für eine weitere Verarbeitung und Datenspeicherung gibt, wie z. B. „zur Erfüllung einer rechtlichen Verpflichtung, die eine Verarbeitung durch das Recht der Union oder eines Mitgliedstaates erfordert, dem der für die Verarbeitung Verantwortliche unterliegt" (Artikel 17 Absatz 3 Buchstabe b)), erkennt die DSGVO an, dass Organisationen zur Speicherung von Daten verpflichtet werden können. Sie sollten jedoch sicherstellen, dass Sie Ihren Rechtsbeistand hinzuziehen, um sicherzustellen, dass die Gründe für die Vorratsspeicherung gegen die Rechte und Freiheiten der betroffenen Personen, ihre Erwartungen zum Zeitpunkt der Datenerhebung usw. abgewogen werden.

Befasst sich die DSGVO mit Verschlüsselung?

Die Verschlüsselung wird in der DSGVO als eine Schutzmaßnahme identifiziert, die personenbezogene Daten unverständlich macht, wenn sie von einer Verletzung betroffen sind. Daher kann sich die Frage, ob eine Verschlüsselung verwendet wird, auf die Anforderungen für die Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten auswirken. Die DSGVO weist auch auf die Verschlüsselung als eine geeignete technische oder organisatorische Maßnahme in einigen Fällen hin, je nach Risiko. Die Verschlüsselung ist auch eine Anforderung durch den Datensicherheitsstandard der Zahlungskartenindustrie und Teil der strengen Compliance-Richtlinien, die speziell für die Finanzdienstleistungsbranche gelten.

Microsoft-Produkte und -Dienstleistungen wie Azure, Dynamics 365, Enterprise Mobility + Security, Office Microsoft 365, SQL Server/Azure SQL-Datenbank, Windows 10 und Windows 11 bieten eine robuste Verschlüsselung der Daten während der Übertragung und der Daten im Ruhezustand.

Wie verändert die DSGVO die Reaktion einer Organisation auf Verletzungen des Schutzes personenbezogener Daten?

Die DSGVO wird die Datenschutzanforderungen ändern und strengere Verpflichtungen für Verarbeiter und für die Verarbeitung Verantwortliche in Bezug auf die Meldung von Verletzungen des Schutzes personenbezogener Daten vorsehen. Gemäß der neuen Verordnung muss der Verarbeiter den für die Verarbeitung Verantwortlichen über eine Verletzung des Schutzes personenbezogener Daten informieren, nachdem er davon Kenntnis erhalten hat, und zwar ohne unangemessene Verzögerung. Sobald der für die Verarbeitung Verantwortliche Kenntnis von einer Verletzung des Schutzes personenbezogener Daten hat, muss er die zuständige Datenschutzbehörde innerhalb von 72 Stunden benachrichtigen. Wenn die Verletzung wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten des Einzelnen führen wird, müssen die Verantwortlichen die betroffenen Personen ebenfalls unverzüglich benachrichtigen. Zusätzliche Leitlinien zu diesem Thema werden von der Arbeitsgruppe des Artikels 29 der EU entwickelt.

Microsoft-Produkte und -Dienstleistungen, wie Azure, Dynamics 365, Enterprise Mobility + Security, Microsoft Office 365 und Windows 10, stehen heute zur Verfügung, um Sie bei der Erkennung und Bewertung von Sicherheitsbedrohungen und Sicherheitsverletzungen zu unterstützen und die DSGVO-Benachrichtigungspflichten zu erfüllen.

Weitere Ressourcen

- Sprechen Sie Ihre Bedürfnisse rund um DSGVO mit einem unserer globalen Partner an, der Microsoft-basierte Lösungen anbietet.
- Erfahren Sie, wie Microsoft Ihre Daten verwaltet, wo sie sich befinden, wer auf sie und die Bedingungen zugreifen kann und vieles mehr.
- Wie Microsoft im Rahmen der DSGVO Verletzungen des Schutzes personenbezogener Daten erkennt, darauf reagiert und Sie darüber informiert
- Bewerten Sie Ihre DSGVO-Bereitschaft noch heute