

# Datenschutzkonforme Nutzung von Microsoft 365

Juni | 2025



Wichtige Datenschutzinformationen für Ihr Unternehmen

## *Inhaltsverzeichnis*

Begrüßung   Ihr Datenschutzbeauftragter vor Ort _____	3
Warum Datenschutz bei Microsoft 365 sehr wichtig ist? _____	4
Bedeutung der DSGVO für Unternehmen _____	4
Herausforderungen bei der Nutzung von Cloud-Diensten _____	5
Vertragsprüfung und rechtliche Grundlagen _____	6
Auftragsverarbeitungsverträge mit Microsoft _____	6
Standardvertragsklauseln und Datenübermittlung in Drittländer _____	7
Transparenz und Dokumentation _____	8
Nachvollziehbarkeit der Datenflüsse _____	8
Nutzung von Microsoft-Tools zur Datenverarbeitung _____	9
Datenschutz-Folgenabschätzung (DSFA) _____	10
Notwendigkeit und Durchführung einer DSFA _____	10
Bewertung und Minimierung von Risiken _____	11
Technische und organisatorische Maßnahmen _____	12
Sicherheitsfeatures wie Multi-Faktor-Authentifizierung _____	12
Regelmäßige Sicherheitsüberprüfungen und Audits _____	13
Datenschutzfreundliche Konfiguration _____	14
Voreinstellungen und risikominimierende Maßnahmen _____	14
Einschränkung der Datenverarbeitung durch Microsoft _____	15
Schulungen und Sensibilisierung des Personals _____	16
Training für Mitarbeiter zur sicheren Nutzung von Microsoft 365 _____	16
Umgang mit personenbezogenen Daten _____	17
Zusammenarbeit mit Datenschutzexperten _____	18
Unterstützung bei der Implementierung datenschutzkonformer Lösungen _____	18
Beratung zur Einhaltung der DSGVO-Vorgaben   Schlusswort _____	19
Impressum _____	20

## Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Liebe Leserin, lieber Leser,

mit Microsoft 365 hat der Technologiegigant den wohl meist genutzten Cloud-Dienst der Welt und somit ist dieser automatisch auch bei vielen deutschen und europäischen Firmen sehr beliebt. Die Flexibilität und Skalierbarkeit, die Arbeitsplatzunabhängige Zusammenarbeit und Kommunikation, die Integration von künstlicher Intelligenz und die Möglichkeit einer plattformübergreifenden Nutzung sind nur wenige Vorteile, die für den Einsatz dieser fortschrittlichen Technologien sprechen.

Betrachtet man das Ganze allerdings aus der Sicht des Datenschutzes und der Datenschutzgrundverordnung (DSGVO), kommen bei der Nutzung des Cloud-Dienstes dann doch erhebliche Bedenken auf. Beispielsweise kam der *Zusammenschluss der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder in Deutschland (Datenschutzkonferenz (DSK))* jetzt schon mehrfach zu dem Schluss, dass Microsoft 365 auf Basis der vorgelegten Dokumente nicht datenschutzkonform betrieben werden kann! Zudem stuft die DSK die Nutzung als „Risikoentscheidung“ ein, was zur Folge hat, dass Unternehmen beim Einsatz von Microsoft 365, die volle Verantwortung für die datenschutzkonforme Nutzung übernehmen müssen. Somit sollte jedes Unternehmen prüfen, in wie weit man mit einer *Datenschutz-Folgenabschätzung*, einem *Transfer Impact Assessment* und einem *Legitimate Interests Assessment* die Risiken minimieren kann.

Nimmt man alle Informationen zusammen, dann bietet die Nutzung von Microsoft 365 sehr viele Vorteile, sie bringt aber auch einige datenschutzrechtliche Risiken mit sich, die zwingend beachtet und minimiert werden müssen.

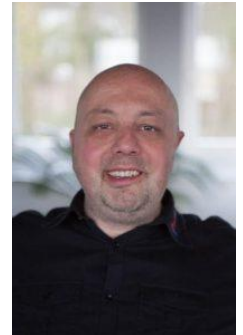
Um auch Ihnen einen ersten Überblick zur „Datenschutzkonformen Nutzung von Microsoft 365“ zu geben, haben wir das Thema in dieser Datenschutzzeitung in den Fokus gestellt. Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung in Anspruch nehmen wollen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung.

Sie erreichen uns unter der Telefonnummer 06894-38797-0 oder per E-Mail an [info@compusaar.de](mailto:info@compusaar.de).

Mit besten Grüßen

**Christoph Hildmann**

Externer Datenschutzbeauftragter



*Alexander Eich*



*Christoph Hildmann*

# Warum Datenschutz bei Microsoft 365 sehr wichtig ist



## Allgemeines

Die Nutzung von Microsoft 365 ist aus dem Arbeitsalltag vieler Unternehmen nicht mehr wegzudenken. Als cloudbasiertes Softwarepaket bietet es zahlreiche Vorteile wie Flexibilität, Skalierbarkeit und Effizienz. Doch gerade im Hinblick auf den Datenschutz stellen sich viele Fragen, u. a. warum Datenschutz bei der Nutzung von Microsoft 365 so entscheidend ist?

Die folgenden Informationen sollen Ihnen einen ersten Überblick über die Bedeutung der Datenschutzgrundverordnung (DSGVO) und den Herausforderungen bei der Nutzung von Cloud-Diensten vermitteln.

## Bedeutung der Datenschutzgrundverordnung (DSGVO) für Unternehmen

Die DSGVO ist seit Mai 2018 in Kraft und regelt den Schutz personenbezogener Daten innerhalb der EU. Sie stellt hohe Anforderungen an Unternehmen und hat das Ziel, Datenmissbrauch zu verhindern und die Rechte Betroffener zu stärken.

Für Unternehmen bedeutet dies:

- **Rechenschaftspflicht**  
Sie müssen nachweisen können, dass sie personenbezogene Daten rechtmäßig verarbeiten.
- **Transparenz**  
Kunden, Lieferanten und Angestellte müssen klar informiert werden, welche Daten verarbeitet werden und zu welchem Zweck.
- **Sanktionen bei Verstößen**  
Hohe Bußgelder und Imageschäden drohen bei Nichteinhaltung der Vorschriften.

Microsoft 365 bietet zwar umfangreiche Sicherheitsmaßnahmen und DSGVO-konforme Vertragsbedingungen, doch die Verantwortung für die Einhaltung der Datenschutzvorgaben liegt letztlich immer beim Unternehmen selbst.

Es reicht nicht aus, sich auf Standardverträge zu verlassen, vielmehr müssen Datenflüsse, Verarbeitungsprozesse und mögliche Risiken sorgfältig geprüft und dokumentiert werden!

# Warum Datenschutz bei Microsoft 365 sehr wichtig ist

## Herausforderungen bei der Nutzung von Cloud-Diensten

Die Nutzung von Cloud-Diensten wie Microsoft 365 birgt neben den Vorteilen auch erhebliche Herausforderungen:

- **Datenschutzverletzungen**  
Cloud-Dienste erhöhen die Angriffsfläche für Cyberangriffe und Datendiebstahl.
- **Komplexität des Shared-Responsibility-Modells**  
Oft ist unklar, welche Sicherheitsaufgaben beim Anbieter und welche beim Unternehmen liegen.
- **Regulatorische Anforderungen**  
Unterschiedliche Datenschutzgesetze in Europa und den USA erschweren die Einhaltung der Vorschriften. Hinzu kommt die politisch unsichere Datenschutz-Lage, die durch die neue Regierung der USA deutlich verschärft wurde. Hier gilt es zu beobachten, ob sich kurzfristig Datenschutzrichtlinien ändern und sich damit möglicherweise Konflikte zur europäischen Datenschutzgrundverordnung (DSGVO) ergeben.
- **Technische Risiken**  
Fehlkonfigurationen, unsichere APIs oder Schatten-IT können Sicherheitslücken schaffen.

Zusätzlich bleibt die Frage offen, wie Microsoft mit personenbezogenen Daten umgeht. Die Datenschutzkonferenz (DSK) hat hier mehrfach betont, dass Microsofts Maßnahmen noch nicht ausreichen, um eine vollständige DSGVO-Konformität sicherzustellen. Unternehmen müssen daher eigene Maßnahmen ergreifen, wie z. B. die Verschlüsselung sensibler Daten oder die detaillierte Dokumentation aller Verarbeitungsprozesse.

Datenschutz ist kein optionales Add-on, sondern eine zentrale Verpflichtung für jedes Unternehmen. Die Nutzung von Microsoft 365 erfordert somit ein tiefes Verständnis der DSGVO sowie eine aktive Auseinandersetzung mit den spezifischen Herausforderungen von Cloud-Diensten. Überwacht werden müssen auch politischen Anpassungen von Datenschutzrichtlinien, die einen Konflikt zur DSGVO darstellen könnten.

Nur so können Unternehmen sicherstellen, dass sie rechtlich auf der sicheren Seite stehen und das Vertrauen ihrer Kunden, Lieferanten und Angestellten rechtfertigen.

# Vertragsprüfung und rechtliche Grundlagen

## *Vertragsprüfung und rechtliche Grundlagen*

Die datenschutzkonforme Nutzung von Microsoft 365 stellt Unternehmen vor rechtliche Herausforderungen, insbesondere bei der Vertragsgestaltung und der Datenübermittlung.

Folgend sollen die wesentlichen Aspekte der *Auftragsverarbeitungsverträge mit Microsoft* und den *Standardvertragsklauseln für Datenübermittlungen in Drittländer* beleuchtet werden.

### Auftragsverarbeitungsverträge mit Microsoft

Gemäß Artikel 28 DSGVO müssen Unternehmen sicherstellen, dass ihre Auftragsverarbeiter, in diesem Beispiel Microsoft, hinreichende Garantien für die Einhaltung der Datenschutzvorgaben bieten, u. a. der Datenschutzgrundverordnung (DSGVO).

Microsoft agiert hierbei als Auftragsverarbeiter und verarbeitet personenbezogene Daten in seinen weltweit verfügbaren Rechenzentren.

### Die Standard-Auftragsverarbeitungsvereinbarung reicht nicht aus!

Die Standard-Auftragsverarbeitungsvereinbarung von Microsoft (Data Protection Addendum, DPA) erfüllt nicht vollumfänglich die Anforderungen der Datenschutzbehörden und steht somit in der Kritik:

- **Kritikpunkte**

Die Datenschutzkonferenz (DSK) hat festgestellt, dass die Standardvereinbarung von Microsoft nicht vollständig den Anforderungen des Artikels 28 Abs. 3 DSGVO entspricht.

Problemfelder sind unter anderem die Weisungsbindung, die Offenlegung verarbeiteter Daten und die Umsetzung technischer und organisatorischer Maßnahmen.

- **Empfehlungen**

Unternehmen sollten die Vereinbarung sorgfältig prüfen und gegebenenfalls Anpassungen verlangen. Eine Handreichung der Datenschutzaufsichtsbehörden bietet Unterstützung, um datenschutzkonforme Änderungen durchzusetzen.

Zudem ist es wichtig, alle relevanten Dokumente zu speichern und ein Verzeichnis der Verarbeitungstätigkeiten zu führen.

## Standardvertragsklauseln und Datenübermittlung in Drittländer

Die Übertragung personenbezogener Daten in Länder außerhalb des Europäischen Wirtschaftsraums (EWR) ist ein zentraler Aspekt bei der Nutzung von Microsoft 365.

Nach dem Urteil des Europäischen Gerichtshofs (EuGH) im Juli 2020, das das EU-US-Datenschutzschild für ungültig erklärte, stellen die EU-Standardvertragsklauseln (SCC) den primären Mechanismus für solche Übermittlungen dar.

- **Der Ansatz von Microsoft**

Microsoft implementiert die EU-Standardvertragsklauseln (SCC) in seinen Verträgen, um sicherzustellen, dass personenbezogene Daten gemäß DSGVO verarbeitet werden.

Das Unternehmen bietet zusätzliche Garantien wie *Transfer Impact Assessments (TIA)*, um Risiken bei Drittlandsübermittlungen auf ein Minimum zu reduzieren.

- **Herausforderungen**

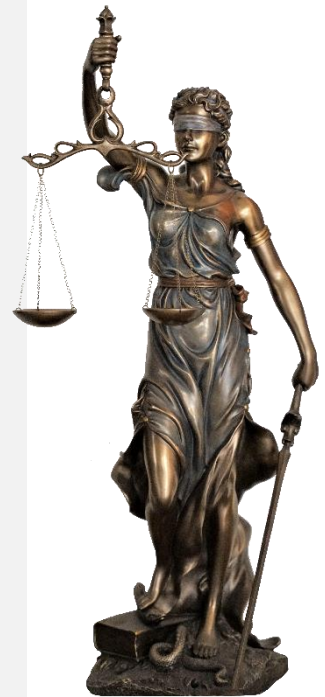
Trotz dieser Maßnahmen bleibt die Einhaltung der DSGVO in der Verantwortung jedes einzelnen Unternehmens.

Es ist erforderlich, die Datenflüsse genau zu dokumentieren und mögliche Risiken durch US-amerikanische Zugriffsrechte zu bewerten.

Die Vertragsprüfung und die Einhaltung rechtlicher Vorgaben bei der Nutzung von Microsoft 365 erfordert eine proaktive Rolle der Unternehmen.

Neben einer sorgfältigen Prüfung der Auftragsverarbeitungsverträge sollten Unternehmen auch die Datenübermittlung in Drittländer kritisch hinterfragen und immer dokumentieren.

Nur so kann eine datenschutzkonforme Nutzung von Microsoft 365 dauerhaft gewährleistet werden!



# Transparenz und Dokumentation



## Allgemeines

Die datenschutzkonforme Nutzung von Microsoft 365 erfordert eine klare Strategie die eine maximale Transparenz und eine umfassende Dokumentation in den Mittelpunkt stellt.

Unternehmen sind hierbei verpflichtet, die Datenflüsse innerhalb ihrer Systeme nachvollziehbar zu machen und geeignete Microsoft-Tools für die Datenverarbeitung zu nutzen.

## Nachvollziehbarkeit der Datenflüsse

Die Datenschutzgrundverordnung (DSGVO) fordert von Unternehmen, dass sie sämtliche Datenflüsse innerhalb ihrer Organisation dokumentieren und nachvollziehbar gestalten.

Dies umfasst:

- **Identifikation der Datenquellen**  
Unternehmen müssen klar definieren, welche personenbezogenen Daten verarbeitet werden und woher diese stammen.
- **Analyse der Datenströme**  
Es ist essenziell, den Weg der Daten durch verschiedene Systeme zu verfolgen, einschließlich Speicherung, Verarbeitung und Weitergabe an Dritte.
- **Überprüfung der Rechtsgrundlagen**  
Für jede Verarbeitungstätigkeit muss eine rechtliche Grundlage bestehen, wie beispielsweise Einwilligungen oder berechtigte Interessen.
- **Berücksichtigung von Drittlandübermittlungen**  
Wenn Daten außerhalb der EU verarbeitet werden, müssen Mechanismen wie Standardvertragsklauseln oder Datenschutzfolgenabschätzungen implementiert werden.

Microsoft unterstützt Unternehmen dabei mit Berichten und Tools, die Transparenz schaffen. Diese ermöglichen es Verantwortlichen, die Verarbeitungstätigkeiten zu dokumentieren und gegenüber Aufsichtsbehörden nachzuweisen.

## Nutzung von Microsoft-Tools zur Datenverarbeitung

Microsoft 365 bietet zahlreiche Funktionen, die Unternehmen bei der datenschutzkonformen Nutzung unterstützen.

Zu den wichtigsten Tools gehören:

- **Power BI**  
Dieses Tool ermöglicht die Visualisierung und Analyse von Datenströmen. Es bietet umfassende Einblicke in die Verarbeitung personenbezogener Daten und unterstützt bei der Erstellung transparenter Berichte.
- **Microsoft Compliance Center**  
Hier können Unternehmen ihre Datenschutzrichtlinien zentral verwalten, Risiken identifizieren und Maßnahmen zur Einhaltung der DSGVO umsetzen.
- **Microsoft Teams und SharePoint**  
Diese Anwendungen bieten Funktionen zur sicheren Zusammenarbeit und zum Austausch von Dokumenten.  
Sie ermöglichen es, Zugriffsrechte präzise zu steuern und sensible Informationen zu schützen.
- **Microsoft Graph**  
Ermöglicht eine sichere Echtzeit-Datenverarbeitung durch KI-Assistenten wie Microsoft Copilot, wobei strenge Datenschutzmaßnahmen umgesetzt werden.

Darüber hinaus stellt Microsoft sicher, dass die Verarbeitung personenbezogener Daten in Übereinstimmung mit den geltenden Datenschutzbestimmungen erfolgt. Funktionen wie *Multi-Faktor-Authentifizierung*, *Verschlüsselung* und *Bedrohungserkennung* tragen zudem dazu bei, Sicherheitsrisiken zu minimieren.

Transparenz und Dokumentation sind zentrale Elemente für die datenschutzkonforme Nutzung von Microsoft 365. Durch die Kombination aus klarer Nachvollziehbarkeit der Datenflüsse und dem gezielten Einsatz von Microsoft-Tools können Unternehmen ihre DSGVO-Verpflichtungen erfüllen und das Vertrauen von Kunden, Lieferanten und Angestellten stärken.

# Die Datenschutz-Folgenabschätzung (DSFA)



## Allgemeines

Die Datenschutz-Folgenabschätzung (DSFA) ist ein essenzielles Instrument zur Sicherstellung der datenschutzkonformen Nutzung von Microsoft 365. Sie dient dazu, die Risiken für die Rechte und Freiheiten natürlicher Personen zu bewerten und zu minimieren, die durch die Verarbeitung personenbezogener Daten entstehen können.

## Notwendigkeit und Durchführung einer Datenschutz-Folgenabschätzung

Gemäß Artikel 35 der Datenschutzgrundverordnung (DSGVO) ist eine Datenschutz-Folgenabschätzung (DSFA) immer dann erforderlich, wenn die Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt.

Typische Szenarien, die eine DSFA notwendig machen, sind:

- Systematische und umfassende Bewertung persönlicher Aspekte mittels automatisierter Verarbeitung, einschließlich Profiling.
- Umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten, wie Gesundheitsdaten oder politische Meinungen.
- Systematische Überwachung öffentlich zugänglicher Bereiche.

Für Unternehmen, die Microsoft 365 einsetzen, ist es entscheidend, zunächst eine sogenannte Schwellenwertanalyse durchzuführen. Diese Analyse hilft zu bestimmen, ob eine DSFA notwendig ist. Dabei sind Faktoren wie Art, Umfang und Zweck der Datenverarbeitung zu berücksichtigen.

Eine gründliche Datenschutz-Folgenabschätzung (DSFA) umfasst unter anderem folgende Schritte:

- **Identifikation der Verarbeitungsvorgänge**  
Erfassung aller relevanten Datenflüsse innerhalb von Microsoft 365.
- **Bewertung der Risiken**  
Analyse potenzieller Gefahren für die betroffenen Personen.
- **Dokumentation**  
Schriftliche Festhaltung der Ergebnisse und Maßnahmen zur Risikominimierung.

# Die Datenschutz-Folgenabschätzung (DSFA)

## Bewertung und Minimierung von Risiken

Die Datenschutz-Folgenabschätzung (DSFA) ermöglicht eine systematische Bewertung der Risiken und bietet Ansätze zur Minimierung potentieller Gefahren. Für Microsoft 365 können folgende Maßnahmen ergriffen werden:

- **Technische Anpassungen**  
Konfiguration von Sicherheitsmaßnahmen wie Verschlüsselung und Zugriffskontrollen.
- **Organisatorische Maßnahmen**  
Schulung der Mitarbeiter im Umgang mit sensiblen Daten und Implementierung klarer Richtlinien zur Datenverarbeitung.
- **Rechtliche Absicherung**  
Abschluss von Standardvertragsklauseln mit Microsoft zur Sicherstellung des Schutzes personenbezogener Daten bei internationalen Datentransfers.

Ein besonders wichtiger Aspekt ist die regelmäßige Überprüfung der implementierten Maßnahmen sowie die Anpassung an neue rechtliche Vorgaben oder technologische Entwicklungen. Durch diese kontinuierliche Optimierung können Unternehmen sicherstellen, dass die Nutzung von Microsoft 365 den Anforderungen der Datenschutzgrundverordnung (DSGVO) entspricht und mögliche Bußgelder vermieden werden.

Die Datenschutz-Folgenabschätzung ist ein unverzichtbarer Prozess für Unternehmen, die Microsoft 365 einsetzen. Sie hilft nicht nur dabei, datenschutzrechtliche Risiken zu erkennen und zu minimieren, sondern trägt auch wesentlich zur Schaffung von Vertrauen bei Kunden, Lieferanten und Angestellten bei.

Eine sorgfältige Durchführung der Datenschutz-Folgenabschätzung (DSFA) ist daher ein wichtiger Schritt hin zu einer sicheren und rechtskonformen Nutzung von Microsoft 365.

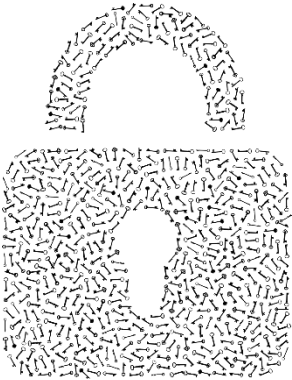
Empfehlung

Beachten Sie hierzu unsere Datenschutzzeitung zum Thema:

„*Datenschutz-Folgenabschätzung (DSFA)*“



## Technische und organisatorische Maßnahmen



### *Allgemeines*

Die datenschutzkonforme Nutzung von Microsoft 365 erfordert die Implementierung technischer und organisatorischer Maßnahmen (TOM), um die Sicherheit personenbezogener Daten zu gewährleisten.

Diese Maßnahmen sind nicht nur essenziell für die Einhaltung der Datenschutzgrundverordnung (DSGVO), sondern auch für den Schutz sensibler Unternehmensinformationen.

### **Sicherheitsfeatures wie Multi-Faktor-Authentifizierung (MFA)**

Die Multi-Faktor-Authentifizierung ist eine der effektivsten Methoden, um unbefugten Zugriff auf Microsoft 365-Konten zu verhindern. Sie bietet eine zusätzliche Sicherheitsebene, indem sie neben dem Passwort einen zweiten Authentifizierungsfaktor verlangt.

Beispiele:

- **Einmalpasswörter**  
Diese werden per SMS oder App generiert und sind nur für kurze Zeit gültig.
- **Biometrische Daten**  
Fingerabdruck- oder Gesichtserkennung können als zweiter Faktor dienen.
- **Hardware-Token**  
Physische Geräte, die einen Authentifizierungscode bereitstellen können die Sicherheit der Konten deutlich erhöhen.

Durch die Aktivierung der Multi-Faktor-Authentifizierung (MFA) können Unternehmen das Risiko von Phishing-Angriffen und kompromittierten Anmeldedaten erheblich reduzieren.

Microsoft bietet in seinem Admin Center einfache Konfigurationsmöglichkeiten für die Einrichtung der Multi-Faktor-Authentifizierung (MFA), die jedes Unternehmen nutzen sollten.

## Technische und organisatorische Maßnahmen

### Regelmäßige Sicherheitsüberprüfungen und Audits

Regelmäßige Sicherheitsüberprüfungen und Audits sind entscheidend, um Schwachstellen im System frühzeitig zu erkennen und zu beheben.

Hierzu gehören unter anderem folgende Maßnahmen:

- **Penetrationstests**  
Externe Sicherheitsexperten simulieren Angriffe, um potenzielle Sicherheitslücken aufzudecken.
- **Überprüfung der Berechtigungskonzepte**  
Stellen Sie sicher, dass nur autorisierte Personen Zugriff auf sensible Daten haben.
- **Protokollierung und Monitoring**  
Überwachen Sie Zugriffsprotokolle und Aktivitäten in Microsoft 365, um verdächtige Vorgänge zu identifizieren.
- **Datenschutz-Folgeabschätzungen (DSFA)**  
Diese sind erforderlich, wenn ein hohes Risiko für die Rechte und Freiheiten von Personen besteht.

Microsoft unterstützt Unternehmen mit Tools wie dem Compliance Manager, der Checklisten für DSGVO-Anforderungen bereitstellt.

Zudem sollten Unternehmen ihre Datenschutz-Dokumentation regelmäßig aktualisieren, um bei Kontrollen durch Aufsichtsbehörden gut vorbereitet zu sein.

Die Kombination aus technischen Sicherheitsfeatures wie z. B. die Multi-Faktor-Authentifizierung (MFA) und organisatorischen Maßnahmen, wie z. B. die Durchführung regelmäßiger Audits, bildet die Grundlage für eine datenschutzkonforme Nutzung von Microsoft 365.

Unternehmen müssen diese Maßnahmen kontinuierlich anpassen und dokumentieren, um den dynamischen Anforderungen der DSGVO gerecht zu werden.

# Datenschutzfreundliche Konfiguration



## Allgemeines

Microsoft 365 ist für viele Unternehmen ein unverzichtbares Tool, doch die datenschutzkonforme Nutzung erfordert eine sorgfältige Konfiguration.

Die folgenden Maßnahmen helfen dabei, die Datenschutzerfordernungen zu erfüllen und die Risiken zu minimieren.

## Voreinstellungen und risikominimierende Maßnahmen

Eine datenschutzfreundliche Konfiguration beginnt mit der Anpassung der Voreinstellungen.

Hier einige zentrale Schritte:

- **Diagnosedaten minimieren**  
Deaktivieren Sie optionale Diagnosedaten, um die Menge der an Microsoft gesendeten Informationen zu reduzieren.  
Nutzen Sie dafür die Datenschutzsteuerungen in den Einstellungen der Office-Anwendungen.
- **Connected Experiences deaktivieren**  
Funktionen wie die personalisierte Werbung oder automatische Übersetzungen sollten ausgeschaltet werden, da diese nicht DSGVO-konform sind.
- **Customer Lockbox aktivieren**  
Diese Funktion stellt sicher, dass Microsoft nur mit Ihrer Zustimmung auf Daten zugreifen kann. Das ist besonders wichtig, sobald sensible personenbezogener Daten verarbeitet werden.
- **Telemetrie und Firewall-Einstellungen optimieren**  
Reduzieren Sie die Übertragung von Telemetriedaten durch Gruppenrichtlinien oder Registry-Eingriffe.  
Blockieren Sie ausgehende Datenströme direkt an der Firewall.

# Datenschutzfreundliche Konfiguration

## Einschränkung der Datenverarbeitung durch Microsoft

Microsoft verarbeitet Kundendaten oft zu eigenen Zwecken, was datenschutzrechtlich sehr problematisch ist.

Als Unternehmen können Sie hier folgende Gegenmaßnahmen ergreifen:

- **Vertragliche Kontrolle**  
Prüfen Sie den Datenschutznachtrag von Microsoft und dokumentieren Sie alle relevanten Datenflüsse sowie Verarbeitungstätigkeiten gemäß Art. 30 DSGVO.
- **Lokale Speicherung bevorzugen**  
Vermeiden Sie die Ablage sensibler Daten in der Cloud, insbesondere auf OneDrive.  
Nutzen Sie alternative Speicherlösungen oder verschlüsseln Sie Dateien vor dem Upload.
- **Rechteverwaltung etablieren**  
Implementieren Sie ein Berechtigungskonzept, das sicherstellt, dass nur autorisierte Personen Zugriff auf bestimmte Daten haben.
- **Sensibilisierung der Mitarbeitenden**  
Schulen Sie Ihre Teams im Umgang mit personenbezogenen Daten und machen Sie klar, welche Informationen nicht in Cloud-Diensten verarbeitet und gespeichert werden dürfen.
- **Regelwerk für die Nutzung von Microsoft 365**  
Erstellen Sie für Ihr Unternehmen ein datenschutzkonformes Regelwerk für die Nutzung von Microsoft 365, welches für alle Mitarbeitenden bindend ist.

Die datenschutzkonforme Nutzung von Microsoft 365 ist möglich, erfordert jedoch technische und organisatorische Maßnahmen. Eine Kombination aus restriktiven Einstellungen, verschlüsselter Speicherung und klaren Richtlinien für alle Mitarbeitenden hilft Unternehmen, die Anforderungen der DSGVO zu erfüllen und bestehende Risiken deutlich zu minimieren.

# Schulungen und Sensibilisierung des Personals



## Allgemeines

Die datenschutzkonforme Nutzung von Microsoft 365 in Unternehmen erfordert nicht nur technische und organisatorische Maßnahmen, sondern auch eine gezielte Schulung und Sensibilisierung aller Mitarbeiterinnen und Mitarbeiter.

Dieser Ansatz hilft, Risiken deutlich zu minimieren und die Einhaltung der Datenschutzgrundverordnung (DSGVO) sicherzustellen.

## Training für Mitarbeiter zur sicheren Nutzung von Microsoft 365

Eine umfassende Schulung des gesamten Personals ist essenziell, um die sichere Nutzung von Microsoft 365 zu gewährleisten.

Dabei sollten folgende Aspekte berücksichtigt werden:

- **Grundlagen des Datenschutzes**  
Vermittlung der relevanten DSGVO-Vorschriften und deren Bedeutung für die tägliche Arbeit. Ziel ist es, ein Bewusstsein für Datenschutzrisiken zu schaffen und die Verantwortung jedes Einzelnen zu betonen.
- **Technische Funktionen von Microsoft 365**  
Mitarbeiter sollten in der Nutzung spezifischer Sicherheitsfeatures wie Multi-Faktor-Authentifizierung, Datenverschlüsselung und Zugriffskontrollen geschult werden.  
  
Diese Funktionen sind entscheidend, um Daten vor unbefugtem Zugriff zu schützen.
- **Praktische Anwendung**  
Praxisnahe Schulungen, die typische Szenarien aus dem Arbeitsalltag simulieren, helfen den Mitarbeiterinnen und Mitarbeitern, Datenschutzmaßnahmen effektiv umzusetzen.  
  
Sowohl Präsenzs Schulungen als auch eLearning-Module und Awareness-Programme sind hierfür sehr gut geeignet.

## Umgang mit personenbezogenen Daten

Der korrekte Umgang mit personenbezogenen Daten ist ein zentraler Bestandteil der DSGVO-konformen Nutzung von Microsoft 365.

Hierzu gehören:

- **Datenerhebung und -verarbeitung**  
Alle Mitarbeiterinnen und Mitarbeiter müssen verstehen, dass personenbezogene Daten nur für festgelegte und legitime Zwecke erhoben werden dürfen.  
Die Verarbeitung sollte stets transparent dokumentiert werden.
- **Speicherung und Löschung**  
Es ist wichtig, dass Daten nur so lange gespeichert werden, wie es für den jeweiligen Zweck erforderlich ist. Nach Ablauf dieser Frist müssen sie sicher gelöscht werden.
- **Weitergabe an Dritte**  
Die Weitergabe von Daten an externe Dienstleister darf nur unter strengen Bedingungen erfolgen.  
Unternehmen sollten sicherstellen, dass Dienstleister vertraglich verpflichtet sind, die Daten gemäß DSGVO zu verarbeiten.

Schulungen und Sensibilisierungsmaßnahmen sind unverzichtbar, um die datenschutzkonforme Nutzung von Microsoft 365 im Unternehmen sicherzustellen.

Sie fördern nicht nur die Kompetenz des Personals im Umgang mit sensiblen Daten, sondern tragen auch dazu bei, rechtliche Risiken besser erkennen und minimieren zu können.

Zudem stärken sie das Vertrauen in den Datenschutz des Unternehmens.

### Empfehlung

Beachten Sie hierzu unsere Datenschutzzeitung zum Thema:

„Mitarbeiter-Awareness“



## Zusammenarbeit mit Datenschutzexperten



### *Allgemeines*

Die datenschutzkonforme Nutzung von Microsoft 365 stellt Unternehmen vor komplexe Herausforderungen.

Eine effektive Lösung liegt in der Zusammenarbeit mit Datenschutzexperten, die sowohl technische als auch rechtliche Expertise einbringen. Diese Zusammenarbeit kann entscheidend dazu beitragen, die Einhaltung der Datenschutzgrundverordnung (DSGVO) sicherzustellen und Risiken zu minimieren.

### **Unterstützung bei der Implementierung datenschutzkonformer Lösungen**

Datenschutzexperten bieten gezielte Unterstützung bei der Einführung und Optimierung von Microsoft 365. Sie analysieren die Datenflüsse innerhalb des Systems, identifizieren Schwachstellen und entwickeln maßgeschneiderte Lösungen.

Zu den zentralen Maßnahmen gehören:

- **Technische Anpassungen**  
Experten helfen bei der Konfiguration von Sicherheitsfeatures wie Multi-Faktor-Authentifizierung, Verschlüsselung und Zugriffskontrollen.
- **Dokumentation und Transparenz**  
Eine vollständige Dokumentation der Datenverarbeitungsprozesse ist essenziell. Experten unterstützen dabei, die notwendigen Berichte und Nachweise zu erstellen.
- **Datenübermittlung in Drittländer**  
Datenschutzexperten beraten zu Mechanismen wie Standardvertragsklauseln, um den Anforderungen der DSGVO gerecht zu werden.

Durch diese Maßnahmen wird sichergestellt, dass Microsoft 365 nicht nur effizient genutzt, sondern auch rechtlich abgesichert ist.

# Zusammenarbeit mit Datenschutzexperten

## Beratung zur Einhaltung der DSGVO-Vorgaben

Die DSGVO stellt hohe Anforderungen an Unternehmen, insbesondere bei der Verarbeitung personenbezogener Daten. Datenschutzexperten leisten hier wertvolle Unterstützung:

- **Rechtskonforme Vertragsprüfung**  
Experten prüfen Verträge zur Auftragsverarbeitung mit Microsoft, um sicherzustellen, dass sie den DSGVO-Vorgaben entsprechen.
- **Datenschutz-Folgenabschätzung (DSFA)**  
Bei der Verarbeitung sensibler Daten ist eine DSFA erforderlich. Experten bewerten Risiken und entwickeln Strategien zur Risikominderung.
- **Schulungen und Awareness**  
Mitarbeiter werden durch gezielte Schulungen auf die Einhaltung der Datenschutzrichtlinien vorbereitet. Dies stärkt die interne Compliance und minimiert Fehler.

Die Zusammenarbeit mit externen Datenschutzbeauftragten oder spezialisierten Beratungsunternehmen bietet Unternehmen nicht nur rechtliche Sicherheit, sondern auch praktische Lösungen für eine effiziente Nutzung von Microsoft 365. So können Führungskräfte und Mitarbeiter sich auf ihre Kernkompetenzen konzentrieren, während jegliche Datenschutzfragen und Datenschutzaufgaben professionell von externen Datenschutzexperten gelöst werden.

## Schlusswort

Auch wenn die *Datenschutzkonferenz (DSK)* die Nutzung von Microsoft 365 für Unternehmen als „Risikoentscheidung“ eingestuft hat, ist eine datenschutzkonforme Nutzung des Cloud-Dienstes realisierbar.

Allerdings müssen sich Unternehmen bewusst sein, dass für die Datenschutzkonformität einige Maßnahmen getroffen werden müssen. Hierzu zählen eine gewissenhafte Vertragsprüfung, die Umsetzung von technischen und organisatorischen Maßnahmen (TOM) und eine hohe Transparenz und Dokumentationsbereitschaft genauso, wie eine datenschutzfreundliche Konfiguration oder die Schulungen und Sensibilisierung des gesamten Personals.

Sollte zudem eine Datenschutz-Folgenabschätzung (DSFA) notwendig sein, oder eine Rechtsunsicherheit für die Nutzung bestehen, kann es ratsam sein, die Zusammenarbeit mit externen Datenschutzexperten anzustreben.

Unabhängig aller getroffenen Maßnahmen liegt die rechtliche Verantwortung aber immer beim Unternehmen und somit muss jeder eigenverantwortlich entscheiden, ob Microsoft 365 zum Einsatz kommen soll.



## Impressum

### CS Hard- & Software Consulting GmbH

Saarbrücker Straße 72

66386 St. Ingbert

Tel.: 06894 38797 - 0

Fax: 06894 38797 - 99

Web: [www.compusaar.de](http://www.compusaar.de)

E-Mail: [info@compusaar.de](mailto:info@compusaar.de)

Amtsgericht St. Ingbert, HRB 13312

Ust-IdNr.: DE813536236

Geschäftsführer/in: Ursula Doll

### Haftungsausschluss

Mit dieser Broschüre soll ein Überblick über aktuelle Datenschutz-Themen vermittelt werden. Die Informationen haben nicht den Anspruch einer Rechtsberatung. Die Verantwortung liegt immer beim umsetzenden Unternehmen. Eine Haftung für Fehler jeder Art wird ausgeschlossen.

### Redaktion

Alexander Eich

### Bildnachweise

Diese Unterlage wurde in unserem Auftrag von der Firma ITKService GmbH & Co. KG, in 97491 Aidhausen erstellt. Alle verwendeten Bilder sind von <https://pixabay.com/de/> einer Plattform für lizenzfreie Bilder.

### Nutzung von künstlicher Intelligenz

Bei der Recherche und zur Kontrolle der Richtigkeit der Aussagen, wurde bei der Erstellung dieser Unterlage zum Teil auf KI zurückgegriffen.