SPECTRUM Hinweise

Version März 2021

Hinweise zu den technischen Einstellungen bei der Installation durch SPECTRUM von

Microsoft 365 Business Premium

auf SPECTRUM-ASP-Systemen und generelle Sicherheitshinweise beim Einsatz von Microsoft 365

Microsoft bietet mit „Microsoft 365 Business Premium“ ein umfangreiches Paket 1. von lokal installierbaren Programmen (wie Word, Excel, PowerPoint, Outlook, Access, Publisher), 2. von Cloud-Diensten (wie Exchange, Teams, OneNote, OneDrive, SharePoint), 3. von RZ-Services (Apps in der Microsoft-Cloud) und 4. eine Reihe von ergänzenden weiteren Cloud-Anwendungen an (wie z.B. Bookings, Planner, Stream, Sway, Skype for Business usw.). Aus diesem großen Paket kann der Kunde genau jene Dienste und Services auswählen, die er benötigt und nutzen möchte. Dadurch ist es möglich, die IT-Unterstützung seinen Anforderungen genau anzupassen, ohne erst in weitere IT-Infrastrukturen oder weitere Lizenzen investieren zu müssen.

Erfolgreiche Kanzleien und Unternehmen zeichnen sich durch eine offene, flexible und schnelle Zusammenarbeit nicht nur zwischen den eigenen Mitarbeitern aus. Vor allem die Zusammenarbeit mit Mandanten, Kunden, Lieferanten und Partnern ist heute entscheidend - gerade bei Entscheidungsfindungen, Problemlösungen und Services.

Seien Sie weiterhin Vorreiter bei der Digitalisierung Ihres Betriebes!

Mandanten- und Unternehmensdaten sind heute nicht nur ein entscheidender Wettbewerbsvorteil, Schutz von Mandantendaten, Datensicherheit und das Offenbarungsverbot von anvertrauten Informationen sind auch zusätzlich gesetzlich vorgeschrieben. Leider sind diese Daten oft auch von größtem Interesse für Dritte – *gleich welcher Couleur*. Somit sind die permanenten Prüfungen und Kontrollen der technisch-organisatorischen Maßnahmen für die Datensicherheit und den Datenschutz unerlässlich, um das Sicherheitsniveau der Daten und Zugriffe fortlaufend anzupassen und zu optimieren. Microsoft hat hier sicherlich den besten Ruf im Markt, denn ohne höchsten Datenschutz und Datensicherheit würde das gesamte Geschäftsmodell von Microsoft weltweit zusammenbrechen. Microsoft passt nicht nur ständig die technisch-organisatorischen Maßnahmen den neuen Bedrohungsszenarien an, Microsoft hat auch immer in den letzten Monaten auf Bedenken und Anforderungen der europäischen Datenschützer schnell reagiert und auch Terms & Conditions angepasst. Microsoft 365 ist ein Cloud-Dienst von Microsoft, der weltweit über das globale Internet von überall erreichbar ist und somit unterschiedliche Datenschutzstandards und Datenschutzgesetze der diversen Staaten - zum Teil sogar noch mit branchen- oder berufsbezogener Auslegungen - berücksichtigen muss.

Nachdem es viele Monate still um Microsoft 365 und der Datenschutzkonformität nach der europäischen Datenschutzgrundverordnung EU-DSGVO war, poppen in letzter Zeit immer wieder Hiobsbotschaften auf, nach denen die Nutzung von Microsoft 365 kritischer gesehen wird.

Unter „www.spectrum-news.de/diskussionen-zum-microsoft-datenschutz“ finden Sie den chronologischen Verlauf der aktuellen Diskussionen zum Thema Datenschutz & Microsoft 365, dieser Report wird fortlaufend ergänzt.

Unter „www.spectrum-news.de/microsoft-statements-zum-datenschutz“ finden Sie die aktuellen Statements von Microsoft zur EU-DSGVO-Konformität, auch diese Übersicht wird laufend aktualisiert.

In anderen europäischen Staaten ist es hierzu recht ruhig, nur in Deutschland wird das Thema immer wieder hochgekocht. Die Berliner Datenschutzbeauftragte hat sich hier einen besonders kritischen Ruf eingehandelt. Aber auch die deutschen Datenschutzaufsichtsbehörden sind sich bezüglich Microsoft 365 völlig uneins und zerstritten: Ende 2020 ist z.B. ein Unterarbeitskreis der Deutschen Datenschutzkonferenz (DSK – das ist der Zusammenschluss des Bundesdatenschutzbeauftragten mit den Datenschutzbeauftragten der 16 Bundesländer) zu dem Entschluss gekommen, dass sich Microsoft 365 nicht datenschutzkonform einsetzen ließe. Hiergegen hat dann die Aufsichtsbehörde von Bayern umgehend Widerspruch eingelegt und auf der letzten DSK-Sitzung ist die Entscheidung nur denkbar knapp mit neun zu acht Stimmen noch einmal gegen eine generelle Freigabe von Microsoft 365 ausgefallen. Die 17 Mitglieder der DSK sahen zwar noch gemeinsam ein datenschutzrechtliches „Verbesserungspotenzial“ bei Microsoft. Die Minderheit von 8 der 17 Datenschutzbeauftragten (u.a. Bayern, Baden-Württemberg, Hessen, Saarland, Sachsen, Rheinland-Pfalz) kommen aber zu einer anderen Gesamtbewertung als die anderen 9 Datenschützer, weil die Ausarbeitung der Mehrheitsmeinung zu undifferenziert sei und zudem veraltete Vertragsdokumente als Grundlage der Prüfung herangezogen worden waren, die in der Zwischenzeit von Microsoft schon längst nachgebessert wurden. Die Minderheitsmeinung kritisierte u.a. – wie verlautbart wurde - dass Microsoft selbst nicht angehört wurde, was sich in einem rechtsstaatlichen Verfahren jedoch eigentlich gehöre.

Zuvor hatte die bayrische Datenschutzaufsichtsbehörde sogar zu den von Microsoft durchgeführten aktuellen Änderungen der Standardvertragsklauseln folgenden Text veröffentlicht:

> *„Mittlerweile hat Microsoft seine Standardvertragsklauseln um folgende begrüßenswerte Punkte ergänzt:*
>
> - *die Information der betroffenen Person, wenn Microsoft durch eine staatliche Anordnung rechtlich bindend dazu verpflichtet wurde, Daten an US-Sicherheitsbehördenherauszugeben;*
> - *die Verpflichtung von Microsoft, den Rechtsweg zu beschreiten und die US-Gerichte an-zurufen, um die behördliche Anordnung zur Herausgabe der Daten anzufechten*
> - *den Anspruch auf Schadensersatz für die betroffene Person, deren Daten unrechtmäßig verarbeitet wurden und die dadurch einen materiellen oder immateriellen Schaden erlitten hat*
>
> *(https://www.lda.bayern.de/media/pm/pm2020_9.pdf)*

Betrachtet man diese Ausgangslage und möchte man wirklich absolute Rechtssicherheit haben und vollständig rechtssicher agieren, muss man aktuell leider einfach auf den Einsatz von Microsoft 365 verzichten. Das ist leider so …..

Aber dann müsste man auch z.Tl. das Internet abschalten, dürfte nicht mehr telefonieren, keine Telefaxe mehr versenden und nicht mehr am E-Mail-Verkehr teilnehmen.

Jedes kleine Steuerbüro müsste dann auch Fort-Knox-like zu einem Hochsicherheitsbunker umgebaut werden, denn normale Büro- und Haustüren, Fenster mit unter 2 cm dickem Sicherheitsglas erfüllen dann auch nicht mehr die Anforderungen zum Schutz der Akten und der darin enthaltenen Informationen.

> *Betrachtet man das Verhalten der Datenschutzaufsichtsbehörden, kann man das nur als skandalös bezeichnen. Dieser ganze Hick-Hack der behördlichen Datenschützer sorgt für kein bisschen mehr Datensicherheit, verhindert kein Datenleck und keinen Hackerangriff.*

Auch hier gilt aber sicherlich der Grundsatz der Verhältnismäßigkeit.

Wenn Kunden derzeit ihren eigenen Datenschutzbeauftragten zu diesem Thema befragen, dann können die zur eigenen Absicherung und nach diesem diffusen Stand der Diskussion bei den Datenschutzaufsichtsbehörden keinen Freifahrtschein für die Nutzung von Microsoft 365 ausstellen – *einen „Persil-Schein-365“ gibt es leider nicht.*

Jeder Kanzleibesitzer, Geschäftsführer oder Unternehmer muss für sich selbst eine Risiko-Abschätzung für den Einsatz von Microsoft 365 für seinen Betrieb bzw. seine Kanzlei treffen. Nachfolgende SPECTRUM-Ausführungen sollen eine Hilfestellung für die Entscheidungsfindung der Kunden zur Nutzung von Microsoft 365 auf SPECTRUM-ASP-Systemen sein.

Da das Nutzungs- und Anwendungsspektrum von Microsoft 365 sehr weit gefächert ist, muss man das Datenschutz-Thema differenziert betrachten: Man kann z.B. einerseits seine Word-/Excel-Dokumente in der Microsoft-Cloud ablegen und dann von überall per Handy, Tablet, PC schnell auf diese Daten zugreifen, was sicherlich datenschutzrechtlich besonders betrachtet werden sollte. Man kann aber auch die Programme Word und Excel herkömmlich auf seinem SPECTRUM-ASP-System im Hochsicherheits-RZ von SPECTRUM installieren lassen und die Ablage der Word-Excel-Dokumente erfolgt dann auf dem SPECTRUM-ASP-System in seinem eigenen Dokumenten-Management-System.

Das Thema Datenschutz, Datensicherheit und EU-DSGVO-Konformität hängt also stark davon ab, welche Anwendung man überhaupt ob & warum und dann wo & wie aus dem großen Paket von möglichen Anwendungen von Microsoft 365 nutzt.

Unter „www.spectrum-news.de/microsoft-365-anwendungen“ finden Sie alle Anwendungen und Dienste von Microsoft 365 Business Premium“ mit der Information, ob diese Anwendung im SPECTRUM-RZ läuft oder ein Dienst in der Microsoft-Cloud ist, ob diese Programme von SPECTRUM standardmäßig installiert/freigeschaltet werden oder explizit nur auf Kundenanforderung. Hier spricht auch SPECTRUM pro Anwendung eine Nutzungsempfehlung für den Anwender aus. Diese Internet-Information wird fortlaufend ergänzt und aktualisiert.

Bei SPECTRUM-ASP installiert SPECTRUM Word, Excel, PowerPoint, Access, Publisher, Outlook, SQL-Server usw. ausschließlich auf den SPECTRUM-ASP-Servern im Hochsicherheits-Rechenzentrum von SPECTRUM in Düsseldorf. Für diese **Hybride-Cloud-Nutzung** hat Microsoft SPECTRUM eine spezielle QMTH-Autorisierung (**Qualified Multitenant Hoster**) erteilt. Die Anwender können so diese Anwendungen im sicheren ASP-Modus über getunnelte VPN-Verbindungen nutzen, wobei die Datenhaltung von Word, Excel, PowerPoint, Access, Publisher, Outlook, SQL-Server standardmäßig herkömmlich auf den SPECTRUM-ASP-Servern stattfindet, in den entsprechenden ERP-, DATEV-, DMS-, Dokumentenablage-Programmanwendungen usw. und aus Datenschutz-/Sicherheitsgründen sind sogar darüberhinaus noch einige Funktionen von SPECTRUM standardmäßig gesperrt/deaktiviert (siehe nachfolgende Übersicht) und werden nur auf ausdrücklichen Wunsch des Kunden freigeschaltet.

Stellungnahmen von Datenschützern zu solchen Hybrid-Konfigurationen liegen leider derzeit überhaupt noch nicht vor, alle Statements der Datenschutzaufsichtsbehörden beziehen sich bisher nur auf die 100%ige Cloud-Nutzung von Microsoft 365 mit der Speicherung in der Microsoft-Cloud.

Außerdem gibt es von europäischen Datenschützern (primär basierend auf den Datenschutz-Folgeabschätzungen der niederländischen Datenschutz-Aufsichtsbehörde) erstellte und anerkannte Anleitungen und Empfehlungen (diese finden Sie unter „8. Checkliste für notwendige Einstellungen für den datenschutzkonformen Einsatz von Microsoft 365“ ebenfalls auf der SPECTRUM-Homepage unter „Diskussionen zum Microsoft-Datenschutz“). Auf diese Einstellungs-Empfehlungen gehen wir hier nachfolgend ein. Wenn diese Einstellungs-Empfehlungen übernommen werden, besagt das, dass dann die Nutzung von Microsoft 365 EU-DSGVO-konform ist. Diese Einstellungen nimmt SPECTRUM bei jeder Installation von Microsoft 365 Business Premium auf SPECTRUM-ASP-Systemen weitestgehend vor und nachfolgend ist beschrieben, wie SPECTRUM diese Empfehlungen technisch umgesetzt hat.

Umsetzung der europäischen Datenschutz-Empfehlungen zur Nutzung von Microsoft 365:

1. **Empfehlung:** „Die Nutzung von **Connected-Experiences/Services** in Microsoft 365 sollte nach dieser Datenschutz-Empfehlung deaktiviert werden“. Bei den „Connected Experiences“ handelt es sich um Funktionalitäten wie die Rechtschreibprüfung, Spracherkennung, Handschrifterkennung, Übersetzungen oder sonstige Hilfen. Microsoft hält sich hier einerseits für die Bereitstellung einiger dieser Funktionen für einen Auftragsverarbeiter - jedoch sieht sich Microsoft hier andererseits bei einigen dieser Connected-Experiences auch als eigenständiger Verantwortlicher, wodurch die Begrenzung der Verwendungszwecke nach EU-DSGVO nicht mehr greift. Bei einer SPECTRUM-

ASP-Installation von Microsoft 365 deaktiviert SPECTRUM diese Funktionen durch Gruppenrichtlinien bzw. Registry-Einträge auf ASP-Betriebssystem-Ebene. Folgende Connected-Experiences sind somit deaktiviert:

- 3D Maps
- Insert online 3D Models
- Map Chart
- Office Store
- Insert Online Video
- Research
- Researcher
- Smart Lookup
- Insert Online Pictures
- LinkedIn Resume Assistant
- Weather Bar in Outlook
- PowerPoint QuickStarter
- Giving Feedback to Microsoft
- Suggest a Feature

Hinweis: In Microsoft 365 Business Premium Lizenz ist enthalten, dass der Kunde diese auch auf bis zu 5 lokalen PCs, Home-PCs, Notebooks, SmartPhones oder Tabletts installieren kann. Bei einer SPECTRUM-Installation ist eingestellt, dass diese Lizenz nicht von jedem Mitarbeiter ohne Rückfrage selbst genutzt werden kann – diese Lizenzrechte liegen bei dem von SPECTRUM im Microsoft-Lizenz-Portal eingetragenen Hauptverantwortlichen (Geschäftsführer, Kanzleichef, Unternehmer). Werden diese zusätzlichen freien Lizenzen vom Kunden selbst genutzt, müssen diese Sicherheitseinstellungen in Eigenverantwortung selbst vom Kunden vorgenommen werden – ansonsten bestehen hier ggfs. Sicherheitslücken.

2. **Empfehlung:** „In den Einstellungen muss **beim Senden der Diagnosedaten die Option „weder noch“** ausgewählt werden“. Neben den Funktions- und Inhaltsdaten verarbeitet Microsoft – bei den Cloud-Anwendungen von Microsoft 365 - bei der Bereitstellung von Microsoft 365 eine Vielzahl sog. Diagnosedaten. Diese enthalten eine von Microsoft 365 eindeutig generierte ID, mit der sie einem Benutzer eindeutig zugeordnet werden können. Microsoft hat bestätigt, diese Daten NICHT für Profiling, Datenanalyse, Marktforschung oder Werbung einzusetzen. Diese Diagnosedaten umfassen u.a. Client-ID, User-ID, Dauer der Nutzung eines Microsoft-Cloud-Dienstes, Event-ID (z.B. getätigte Aktion wie Speichern, Lesen, Löschen usw.). Nach Intervention der europäischen Datenschutzbehörden bietet Microsoft hier jetzt (ab der Version 1904) die Möglichkeit, die Übermittlung von Diagnosedaten auf folgende Stufen einzustellen: *(1) Optimal, (2) Erforderlich, (3) Keine*. Bei SPECTRUM-Installationen wird hier „(3) keine Übertragung“ standardmäßig eingestellt. Die „Grundsätzlichen verbundenen Erfahrungen“ sind jedoch von SPECTRUM auf „aktiv“ gesetzt, da sonst OneDrive nicht funktioniert.

   Hinweis: Installiert ein Kunde die im Microsoft 365 Paket enthaltenen weiteren Lizenzen auf lokalen PCs, Home-PCs, Notebooks oder Tablets usw., muss er selbst sicherstellen, dass diese Einstellungen vorgenommen werden.

3. **Empfehlung:** „Das **Telemetrie-Niveau** von Microsoft 365 ist auf „weder noch“ zu stellen“. Dies ist eine Einstellung in Windows 10/Windows 2019. Nutzer dürfen ihre Aktivitäten nicht mit der Zeitachsen-Funktion von Windows synchronisieren. Bei einer SPECTRUM-ASP-Installation von Microsoft 365 deaktiviert SPECTRUM diese Funktionen durch Gruppenrichtlinien bzw. Registry-Einträge auf ASP-Betriebssystem-Ebene.

   Hinweis: Installiert ein Kunde die im Microsoft 365 Paket enthaltenen weiteren Lizenzen auf lokalen PCs, Home-PCs, Notebooks oder Tablets, muss er selbst sicherstellen, dass „das Telemetrie-Niveau auf „weder noch“ zu stellen“ ist.

4. **Empfehlung:** „Der **Versand von Daten im Rahmen des Customer Experience Improvement Programms** (CEIP) sollte unterbunden werden“. Die Funktion zur Datenübermittlung an Microsoft zur Verbesserung der Benutzerfreundlichkeit von Microsoft Anwendungen wird bei einer SPECTRUM-ASP-Installation von Microsoft 365 durch SPECTRUM durch Gruppenrichtlinien bzw. Registry-Einträge auf ASP-Betriebssystem-Ebene deaktiviert.

Hinweis: Installiert ein Kunde die im Microsoft 365 Paket enthaltenen weiteren Lizenzen auf lokalen, PCs, Home-PCs, Notebooks oder Tablets usw., muss er selbst sicherstellen, dass dieser Versand von Daten im Rahmen des Customer Experience Improvement Programms (CEIP) unterbunden wird.

5. **Empfehlung:** „Die **LinkedIn-Integration von Mitarbeiterkonten ist zu deaktivieren**“. Dies kann in der Administratoroberfläche eingestellt werden. Derzeit ist die Funktion in Deutschland per Default standardmäßig von Microsoft deaktiviert. Allerdings sollte dies nach Updates überprüft werden, denn es ist nicht ungewöhnlich, dass Microsoft bei Updates Änderungen an solchen Einstellungen vornimmt.

6. **Empfehlung:** Je nach Sensitivität der Daten sollten die Microsoft-Zusatzprodukte **„Customer Lockbox“** oder der **„Customer Key“** verwendet werden. Werden äußerst sensible Daten bzw. Dokumente mit Microsoft 365 in der Microsoft-Cloud bearbeitet, sollte ggfs. die Verwendung der Kunden-Lockbox-Funktion von Microsoft in Betracht gezogen werden - diese stellt eine kundenseitige Verschlüsselung der Dokumente in der Microsoft-Cloud sicher. Diese Empfehlung betrifft jedoch nicht die Daten, die im SPECTRUM-ASP-System gespeichert und verwaltet werden. Diese Empfehlung betrifft nur Daten, die der Anwender selbst in der Microsoft-Cloud speichert. Die Entscheidung über den Einsatz obliegt dem Anwender, es ist hierzu aber der Einsatz der teuren Variante „Microsoft 365 E5“ Voraussetzung.

7. **Empfehlung:** „Sofern **Workplace Analytics** oder **Activity Reports** genutzt werden sollen, ist vor Aktivierung ggf. eine separate Datenschutz-Folgenabschätzung durchzuführen und ggfs. der Betriebsrat in Kenntnis zu setzen. D.h. das Plugin „**Insights**“ sollte dabei standardmäßig nicht installiert werden, da hierbei zusätzliche Informationen für die Analytics-Analyse gesammelt werden“. Bei einer SPECTRUM-ASP-Installation von Microsoft 365 sorgt SPECTRUM dafür, dass diese Funktionen nicht auf dem ASP-System installiert werden und überwacht dies kontinuierlich mit Managed-Service-Tools.

   Hinweis: Installiert ein Kunde die im Microsoft 365 Paket enthaltenen weiteren Lizenzen auf lokalen PCs, Home-PCs, Notebooks oder Tablets, dann muss er selbst sicherstellen, dass Workplace-Analytics oder Activity-Reports nicht installiert werden.

8. **Empfehlung:** „Nutzer sind nach Möglichkeit technisch und **durch interne Richtlinien davon abzuhalten**, Microsoft-Online-Anwendungen oder mobile Microsoft-Applikationen zu verwenden. Microsoft-Cloud-Anwendungen können ggfs. ein hohes datenschutzrechtliches Risiko für Betroffene in sich bergen und die Freigabe der Nutzung sollte vom Geschäftsführer, Kanzleichef, Unternehmer im Einzelfall abgewägt werden. SPECTRUM stellt hierzu pro Anwendung auf der Internetseite „www.spectrum-news.de/microsoft-365-anwendungen-und-dienste“ kontinuierlich aktuelle Informationen zur Verfügung. Diese Empfehlung der Datenschützer schränken die Nutzung von Microsoft 365 in vielen Bereichen ggfs. ein – es muss aber jeder Anwender die Folgen selbst abschätzen. SPECTRUM sieht hier bei Microsoft-Cloud-Anwendungen, die auf Servern in deutschen Rechenzentren von Microsoft laufen, allerdings ein sehr geringes datenschutztechnisches Risiko.

Datenschutz-Folgenabschätzung

Nach EU-DSGVO ist der Anwender von Microsoft 365 ggfs. verpflichtet eine sogenannte Datenschutz-Folgenabschätzung (DSFA) vorzunehmen. Dies ist eine strukturierte Risikoanalyse zur Vorabbewertung der möglichen Folgen von Datenverarbeitungsvorgängen, die in Art. 35 der EU-DSGVO geregelt ist.