# Datenschutz im Home-Office

Oktober | 2020


Wichtige Datenschutzinformationen für Ihr Unternehmen

# Inhalte | Datenschutzinformationen

*Inhaltsverzeichnis*

# Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Liebe Leserin, lieber Leser,

Anfang 2020 hat eine Pandemie weltweit die komplette Arbeitswelt auf den Kopf gestellt. Alles was bis dahin als normal schien, stand plötzlich auf dem Prüfstand. Abstandsregeln, Hygienevorschriften, der Kontakt mit Kunden und Lieferanten, Messen, Konferenzen, Mitarbeiter-Meetings und hunderte Dinge mehr mussten rasend schnell verändert und an die deutlich erschwerten Bedingungen angepasst werden. Alles mit dem Ziel, Mitarbeiter und Kunden vor möglichen Infektionen zu schützen, den laufenden Betrieb sicherzustellen und mit allen notwendigen Maßnahmen das Unternehmen so gut es geht vor größeren Schäden zu bewahren. Viele Firmen haben diese extreme Herausforderung bravourös gemeistert und in Rekordzeit sehr viele Arbeits- und Produktionsprozesse an die neuen Gegebenheiten angepasst.

Eine hierbei viel genutzte Lösung war die Einrichtung von Telearbeitsplätzen, die ein permanentes arbeiten von zu Hause ermöglichen. Ganze Büros wurden von heute auf morgen geräumt und in die Wohnungen der Beschäftigten verlagert. Home-Office war das große Schlagwort, welches überall zu hören war und auch noch lange nach der Pandemie für viele Unternehmen wichtig sein wird.

Nur wie sieht es im Home-Office mit Datenschutz aus? Kann dieser so garantiert werden wie im Unternehmen? Was passiert mit nicht benötigten Unterlagen? Was muss bei Online-Konferenzen und -Meetings beachtet werden? Gibt es erhöhte Risiken für das Unternehmen? …

Da es bezogen auf Tele- oder Home-Office-Arbeitsplätze viele Fragen gibt und Anforderungen zu erfüllen sind, um der Datenschutzgrundverordnung (DS-GVO) gerecht zu werden, haben wir diese Ausgabe unserer Zeitung diesem Thema gewidmet. Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung zum Thema Datenschutz im Allgemeinen wünschen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung.

Sie erreichen uns unter der Telefonnummer + 49 (375) 211 86 279 oder per

E-Mail an info@datenschutz-zwickau.com

Mit besten Grüßen

**Veit Günl**

Betrieblicher und externer Datenschutzbeauftragter (IHK)
Consultant für Datenschutz und Informationssicherheit

# Mobiles Arbeiten und die Auswirkungen auf den Datenschutz

## *Mobiles Arbeiten, Home-Office und Telearbeitsplatz*

Nichts hat in der Zeit der Pandemie so einen Aufschwung erlebt, wie das mobile Arbeiten. Nur was ist mobiles Arbeiten, wie ist ein Home-Office definiert und wie unterscheiden sich diese von einem Telearbeitsplatz?

Starten wir beim mobilen Arbeiten. Ob im Hotel, im Auto, im Urlaub oder Zuhause. Beim mobilen Arbeiten ist man ortsunabhängig mit Hilfe moderner Informations- und Kommunikationstechniken mit der Infrastruktur des Unternehmens verbunden. Einen festen Arbeitsplatz gibt es nicht.

Beim Home-Office spricht man im Allgemeinen von Arbeiten, die gelegentlich außerhalb der normalen Arbeitsumgebung durchgeführt werden, meist im privaten Umfeld der Beschäftigten. Die Vorgaben an einen solchen Arbeitsplatz sind ergonomisch und arbeitsrechtlich eher gering.

Höhere Anforderungen gibt es bei einem Telearbeitsplatz. Hier bildet die regelmäßige Heimarbeit den Standard, welcher vom Arbeitgeber mit seinen Beschäftigten mit vertraglichen Rahmenbedingungen festgelegt werden muss. Auch der Arbeitsplatz und dessen Ausstattung unterliegen hierbei festen Vorgaben, die unter anderem durch das Arbeitsrecht festgelegt sind. Somit ist ein Telearbeitsplatz sowohl ergonomisch als auch in der Ausstattung fast 1:1 vergleichbar mit einem Arbeitsplatz im Unternehmen.

## *Auswirkungen auf den Datenschutz*

Unabhängig davon, ob man mobil arbeitet, gelegentlich im Home-Office tätig ist, oder ob es sich um einen voll ausgestatteten Telearbeitsplatz handelt. Die Vorgaben der Datenschutzgrundverordnung (DS-GVO) müssen immer und überall erfüllt werden, wobei die datenschutzrechtliche Verantwortung immer beim Arbeitgeber bzw. beim Dienstherren liegt!

Eingeschränkte Kontroll- und Einflussmöglichkeiten erschweren die Vorgaben vollumfänglich zu garantieren, zumal die Gefahren eines Datenmissbrauchs oder die, einer unzulässigen Einflussnahme durch Dritte, außerhalb des Unternehmens exponentiell ansteigen.

Ist es beim mobilen Arbeiten meist noch mit einfachen Methoden (Passwortschutz, Verschlüsselung, …) möglich, ein gutes und sicheres Datenschutzniveau herzustellen, so sind die Anforderungen ans Home-Office oder gar an einen Telearbeitsplatz schon deutlich höher. Hier wäre es, neben allen arbeitsrechtlichen Gegebenheiten, für jedes Unternehmen wichtig, mit jedem Beschäftigten eine individuelle Vereinbarung zu treffen, um alle datenschutz- und sicherheitsrelevanten Vorgaben sicherzustellen.

# Datenschutzrechtliche Regelungen im Home-Office

*Datenschutz im Home-Office*

Um auch im Home-Office datenschutzkonform arbeiten zu können, müssen verschiedene Punkte berücksichtigt werden. Diese reichen von einer optimalen Arbeitsumgebung, bis hin zu verschiedenen organisatorischen Regelungen.

Eine gute Orientierungshilfe darüber, was beim Arbeiten außerhalb des Unternehmens im Detail beachtet werden sollte, bietet eine Checkliste, die im Juli 2020 vom bayerischen Landesamt für Datenschutzaufsicht veröffentlicht wurde. Hierbei sind die aufgeführten Prüfpunkte, an denen wir uns orientiert haben, nicht als abschließend zu betrachten, stellen aber einen sehr guten Best-Practice-Ansatz dar, der von der Geschäftsführung oder vom Datenschutzbeauftragten im Sinne einer Soll-Ist-Überprüfung sehr gut verwendet werden kann.

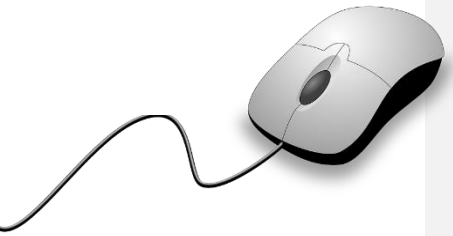
Wichtig: Die Checkliste sollte immer an die individuellen Bedürfnisse des Unternehmens angepasst werden. Dies hat zur Folge, dass manche Punkte gestrichen, andere hingegen hinzugefügt werden müssten. Im Falle einer Streichung sollte dies jedoch kritisch hinterfragt und der Grund samt kurzer Beschreibung dokumentiert werden.

*Der datenschutzkonforme Selbst-Check für das Arbeiten im Home-Office*

**I. Die Arbeitsumgebung**

Die Home-Office-Arbeitsumgebung sollte immer so ausgestaltet sein, dass die Vertraulichkeit und Verfügbarkeit der Daten sichergestellt ist.

- ❑ Der Arbeitsplatz ist so zu wählen, dass weder Familienmitglieder noch Besucher Einblick auf elektronische- und/oder Papierunterlagen erhalten.
- ❑ Bei einer Parterrewohnung, ist der Schreibtisch so zu stellen, dass er nicht von außen einsehbar, bzw. mit einem Sichtschutz verdeckt ist. Zudem sollten beim Verlassen des Arbeitsplatzes immer alle Fenster geschlossen werden.
- ❑ Papierunterlagen mit personenbezogenen Daten sind in Mappen oder Schränken zu verschließen, bzw. mit einem Aktenvernichter zu entsorgen.
- ❑ Auch im Home-Office sollte der PC beim Verlassen des Arbeitsplatzes immer gesperrt werden, falls der Zugriff Dritter – egal ob gewollt oder ungewollt – nicht ausgeschlossen werden kann.
- ❑ Es ist darauf zu achten, dass Telefongespräche nicht von unbefugten Personen mitgehört werden können, sei es z. B. durch eine offene Tür, ein offenes Fenster oder bei einer Videokonferenz.
- ❑ Am Ende des Arbeitstages gilt eine Clean-Desk-Policy (CDP)
  *Hierunter versteht man eine Unternehmensrichtlinie, die das Verlassen des Arbeitsplatzes regelt, z.B., dass keine Papiere zurückgelassen werden dürfen.*



## II. Genutzte Hardware

Bei der Einrichtung eines Home-Office- oder eines Telearbeitsplatzes wird, unter anderem aus Sicherheitsgründen (Viren, Trojaner, Vermischung von geschäftlichen und persönlichen Inhalten, …), eine strikte Trennung zwischen dienstlich und privat genutzter Hardware empfohlen. Privatgeräte, auch als *Bring your own device (BYOD)* benannt, sollten nur in Ausnahmefällen zum Einsatz kommen.

- ❑ Ein dienstlicher Computer (PC / Notebook) wird gestellt.
- ❑ Ein dienstliches Smartphone wir gestellt.
- ❑ Dienstlich zur Verfügung gestellte Geräte werden ausschließlich für dienstliche und nicht für private Zwecke genutzt.
- ❑ Bei Verwendung von Privatgeräten kommen dienstlich eigenständige virtuelle Maschinen zum Einsatz.
- ❑ Bei Verwendung von Privatgeräten werden Remoteverbindungen auf Terminalserver genutzt.

## III. Umgang mit Papierdokumenten

Auch in Unternehmen, in denen der Fortschritt der Digitalisierung sehr hoch ist, gibt es Arbeitsabläufe, bei denen Unterlagen mit personenbezogenen Daten ausgedruckt werden. Beim Umgang mit Papierdokumenten entstehen somit neue Risiken, die in den Räumlichkeiten des Büros normalerweise nicht auftreten. Somit müssen im Home-Office besondere Vorkehrungen getroffen werden, um die datenschutzrechtlichen Vorgaben zu erfüllen. Möglicherweise wird sogar der Einsatz zusätzlicher Hardware notwendig, beispielsweise zur Aktenvernichtung.

- ❑ Papierunterlagen werden in geeigneten Mappen (u. a. mit Name des Unternehmens im Falle eines Verlusts) mit nach Hause genommen.
- ❑ Regelungen bestehen, dass Papierunterlagen beim Transport nach/von zu Hause nicht erhöhten Risikosituationen (z. B. Rücksitz beim Einkaufen, Rucksack im Restaurant) ausgesetzt werden sollen.
- ❑ Entsorgung von Papierunterlagen erfolgt nicht über den eigenen Hausmüll, sondern fachgerecht entweder im Büro oder zu Hause durch einen Aktenvernichter mit mind. Sicherheitsstufe 3 (nach DIN 66399).
- ❑ Es wurde über die Risiken der Schädigung von wichtigen Papierdokumenten (z. B. Kinder bemalen ein Originaldokument) sensibilisiert – es wird bei solchen Dokumenten, sofern möglich, mit Kopien gearbeitet.

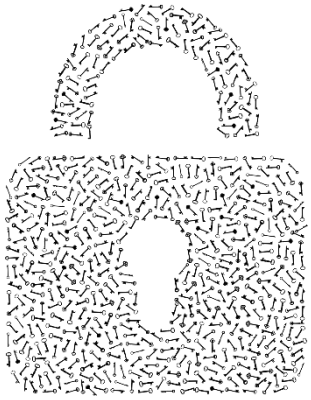
## IV. Nutzung von Videokonferenzsystemen

Auch im Home-Office muss die Kommunikation mit Kollegen, Kunden oder Geschäftspartnern aufrechterhalten werden. Daher ist der Einsatz von Diensten für Video- und Onlinekonferenzen, -Meetings oder Webinaren häufig existenziell.

**Bei der Nutzung dieser Systeme müssen jedoch auch hier die Vorgaben der DS-GVO eingehalten werden, was mit dem Urteil des europäischen Gerichtshofs (EuGH, 16.07.2020) deutlich erschwert wurde. In diesem wurde das sogenannte *Privacy-Shield* für unwirksam erklärt, welches die Basis für alle Datentransfers zwischen der EU und den USA war und jetzt nicht mehr gültig ist! Da aber gleichzeitig viele Marktführer solcher Konferenzsysteme ihren Sitz in der USA haben, ist bei der Nutzung solcher Lösungen besondere Vorsicht geboten!**

Bei der Auswahl eines Systems, mit denen Präsenzbesprechungen teilweise oder vollständig ersetzt werden, müssen viele Anforderungen beachtet werden.

- ❑ Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO ist abgeschlossen.
- ❑ Bei Anbietern in unsicheren Drittstaaten sind geeignete Garantien vorhanden. Beachten Sie hierzu die aktuellen Entwicklungen zur Privacy-Shield-Zertifizierung bei US-Anbietern.
- ❑ Verwendung einer Transportverschlüsselung (z. B. TLS) nach SdT.
- ❑ Verwendung einer Ende-zu-Ende-Verschlüsselung, sofern Daten mit hohem Risiko besprochen bzw. übertragen werden.
- ❑ Zugangsschutz zu Konferenzräumen (Passwörter, individuelle Links).
- ❑ Keine Aufzeichnung der Inhalte durch den Anbieter zum Zweck der Qualitätsverbesserung oder sonstiger Auswertung.
- ❑ Konfigurationsmöglichkeiten bei Erhebung von Telemetriedaten durch den Anbieter (Empfehlung: Deaktivierung).
- ❑ Keine Aufzeichnung der Videokonferenzen durch das Unternehmen.
- ❑ Deaktivierung von biometrischen Features wie Aufmerksamkeitserkennung, sofern eine solche Verarbeitung angeboten wird.
- ❑ Screen Sharing Regelungen sind vorhanden.
- ❑ Regelungen zum Zweck und der Speicherdauer (z. B. Löschung bei Beendigung der Konferenz) von Chat-Funktionen sind vorhanden.
- ❑ Keine Nutzung unzulässiger Tracking-Informationen.
- ❑ Beteiligung des Personal-/Betriebsrats.
- ❑ Beteiligung des Datenschutzbeauftragten.
- ❑ Bei Bedarf: Hintergrund eines Nutzers kann bei Bildübertragung softwareseitig unscharf gestellt werden („Blurring“).
- ❑ Möglichkeit eines virtuellen Warteraumes, in dem Teilnehmer vor Beginn der Konferenz ohne Audio-/Videoübertragung warten können.
- ❑ Es existiert eine Moderator-Funktion zur Konferenz-Steuerung (Screen-Sharing-Option, Stummschaltung, Entfernen von Teilnehmern, …).



## V. Sicherheit

Das eigene Home-Office gilt als virtuelles Büro. Durch die Anbindung ans Internet erhöhen sich die Sicherheitsrisiken enorm. Technische Lösungen helfen, diese Risiken zu minimieren.

- ❑ Anbindung an das Firmennetz mit verschlüsselten VPN-Verbindungen nach Stand der Technik.
- ❑ Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung nebst PIN/ Passwort (z. B. Hardwaretoken oder (Software-) Zertifikate)) bei VPN-Verbindungen.
- ❑ Nutzung vom heimischen WLAN mit starken Passwörtern.
- ❑ Nutzung öffentlicher WLAN-Hotspots nur bei durchgängiger Absicherung sämtlicher Kommunikation durch VPN-Anbindung.
- ❑ Zugriff nur auf für das Home-Office erforderliche Server, Dateiablagen und Anwendungen durch die VPN-Verbindung.
- ❑ Speicherung von Daten auf über die VPN-Verbindung erreichbare Netzlaufwerke im Unternehmen.
- ❑ Ein regelmäßiges Patch Management erfolgt auch auf allen Home-Office-Systemen, u. a. durch Konfiguration automatischer Sicherheitsupdates.
- ❑ Die tägliche Aktualisierung von Virensignaturen ist gewährleistet.
- ❑ Regelungen zum Umgang mit USB-Ports (z. B. Deaktivierung oder Verbot des Anschlusses privater Sticks) wurden getroffen.
- ❑ Festplattenvollverschlüsselung bei Computern.
- ❑ Vollverschlüsselung bei dienstlichen Smartphones.
- ❑ PIN-Sperre bei dienstlichen Smartphones.
- ❑ Regelungen im Verlustfall bei mobilen Endgeräten (z. B. Remote Wipe bei Smartphones, Sperrung von Hardware-Token) wurden getroffen.
- ❑ IT-Abteilung kann bei Fragen und Problemen auch aus dem Home-Office erreicht werden.
- ❑ Einsatz einer Firewall.

## VI. Nutzung von Cloud-Diensten

Im Home-Office setzt die Zusammenarbeit im Team häufig geeignete Softwarewerkzeuge, sogenannte *Collaboration Tools*, voraus. Diese können unter bestimmten Voraussetzungen eingesetzt werden.

- ❑ Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO ist abgeschlossen.
- ❑ Verwendung einer Transportverschlüsselung (z. B. HTTPS) nach Stand der Technik.
- ❑ Ruheverschlüsselung (auf Festplatten des Cloud-Anbieters) nach Stand der Technik.
- ❑ Wirksame Löschung von Daten (z. B. bei Beendigung des Vertrages).
- ❑ Prüffähigkeit der technischen und organisatorischen Maßnahmen durch geeignete Dokumente, Zertifizierungen und zumindest der Möglichkeit, auch ein Vor-Ort-Audit durchzuführen.
- ❑ Bei Anbietern in unsicheren Drittstaaten sind geeignete Garantien vorhanden. Beachten Sie hierzu die aktuellen Entwicklungen zur Privacy-Shield-Zertifizierung bei US-Anbietern.
- ❑ Verwendung starker Passwörter für Nutzer.
- ❑ Verwendung von Verfahren zur Zwei-Faktor-Authentifizierung bei administrativen Konten.
- ❑ Sensibilisierung der Mitarbeiter für Risiken von Phishing-Attacken auf Cloud-Konten.

## VII. Nutzung von Messenger-Diensten

Neben E-Mails werden zunehmend auch Messenger-Systeme für die Unternehmenskommunikation eingesetzt. Diese Dienste müssen für einen aus Datenschutzsicht beanstandungsfreien Einsatz bestimmte Anforderungen erfüllen.

- ❑ Die Kommunikation der Inhalte erfolgt Transport- und Ende-zu-Ende verschlüsselt.
- ❑ Keine Verwendung oder Weitergabe der Verkehrsdaten (wer wann mit wem kommuniziert) an den Anbieter für Zwecke wie Werbung oder Profiling.
- ❑ Ende-zu-Ende-Verschlüsselung auch von Anhängen wie Bildern oder Textnachrichten.
- ❑ Einsatz einer Mobile-Device-Management Lösung zur Steuerung von Kontakt-Uploads an Messenger-Anbieter.

**VIII. Allgemeine organisatorische Regelungen**

Die Anbindung von Mitarbeitern im Zu-Hause-Modus muss durchdacht und sicher ausgestaltet werden. Neben technischen Lösungen helfen organisatorische Regelungen, um Einfallstore für tiefgreifende Cyberangriffe zu verhindern.

- ❑ Überblick über alle Mitarbeiter/innen im Home-Office.
- ❑ Überblick über alle Geräte die vom Personal im Home-Office verwendet werden.
- ❑ Schulung aller Mitarbeiter/innen über alle Home-Office-Regelungen.
- ❑ Schriftliche Verpflichtung der Mitarbeiter/innen, dass diese sich an die Regelungen halten – eine Vor-Ort-Kontrolle kann so i. d. R. entfallen.
- ❑ Keine Weiterleitung von dienstlichen E-Mails an private E-Mail-Konten.
- ❑ Bei sensitiven Dokumenten verhindern Regelungen zum Ausdruck von Dokumenten auf den Druckern im Büro die Einsicht durch unberechtigte.

## *Fazit*

An der sehr umfangreichen Prüfliste der vorangegangenen Seiten ist deutlich zu erkennen, dass sehr viele Parameter beachtet werden müssen, um einen Home-Office- oder einen Telearbeitsplatz zu 100% datenschutzkonform zu betreiben.

Zudem hat das Urteil des europäischen Gerichtshofs (EuGH, 16.07.2020) die Nutzung von Cloud- und Videokonferenzlösungen, die ihren Sitz in den USA haben, deutlich erschwert, weil es fast alle Marktführer solcher Lösungen betrifft.

## *Empfehlung*

Falls auch Sie in Ihrem Unternehmen Mitarbeiter/innen haben, die im Home-Office tätig sind, dann prüfen Sie Ihre Prozesse, so dass eine datenschutzkonforme Tätigkeit außerhalb des Bürogebäudes gewährleistet werden kann. Nutzen Sie hierfür gerne die oben benannte Liste und passen Sie diese genau auf Ihre individuellen Bedürfnisse an.

Erstellen Sie Dokumente, in denen die Tätigkeiten im Home-Office oder beim mobilen Arbeiten genau geregelt sind und verankern Sie dort alle für den Datenschutz relevanten Parameter.

Sensibilisieren Sie Ihre Mitarbeiter/innen auf die speziellen Herausforderungen, die an das mobile Arbeiten außerhalb des Unternehmens geknüpft sind.

## *Datenschutzrechtliche Bedenken bei der Nutzung von Microsoft 365!*

Parallel zur rasanten Zunahme von Home-Office- oder Telearbeitsplätzen, stiegen auch die Nutzerzahlen von Microsoft 365 extrem an. Der Clouddienst erlaubt es über das Internet zu chatten, zu telefonieren, Onlinebesprechungen durchzuführen, oder eine Zusammenarbeit an Dokumenten in Echtzeit - und das alles im Unternehmen oder aus der Ferne. Auf den ersten Blick die optimale Lösung für mobiles Arbeiten.

Allerdings wird die Nutzung der Microsoft 365 Diensten von vielen Datenschützern kritisch gesehen. Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben dahingehend sogar einen Arbeitskreis gebildet, der *„die dem Einsatz des Produktes Microsoft Office 365 zu Grunde liegenden Online Service Terms (OST) sowie die Datenschutzbestimmungen für Microsoft Onlinedienste (Data Processing Addendum / DPA) – jeweils Stand: Januar 2020“* geprüft hat.

***Der Arbeitskreis kam zu dem Ergebnis, dass „auf Basis der genannten Unterlagen kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich ist“.***

Das wiederum haben nicht alle so gesehen und so kam es zu einer Mehrheitsentscheidung, die mit einer Zustimmung von 9:8 Stimmen denkbar knapp ausging.

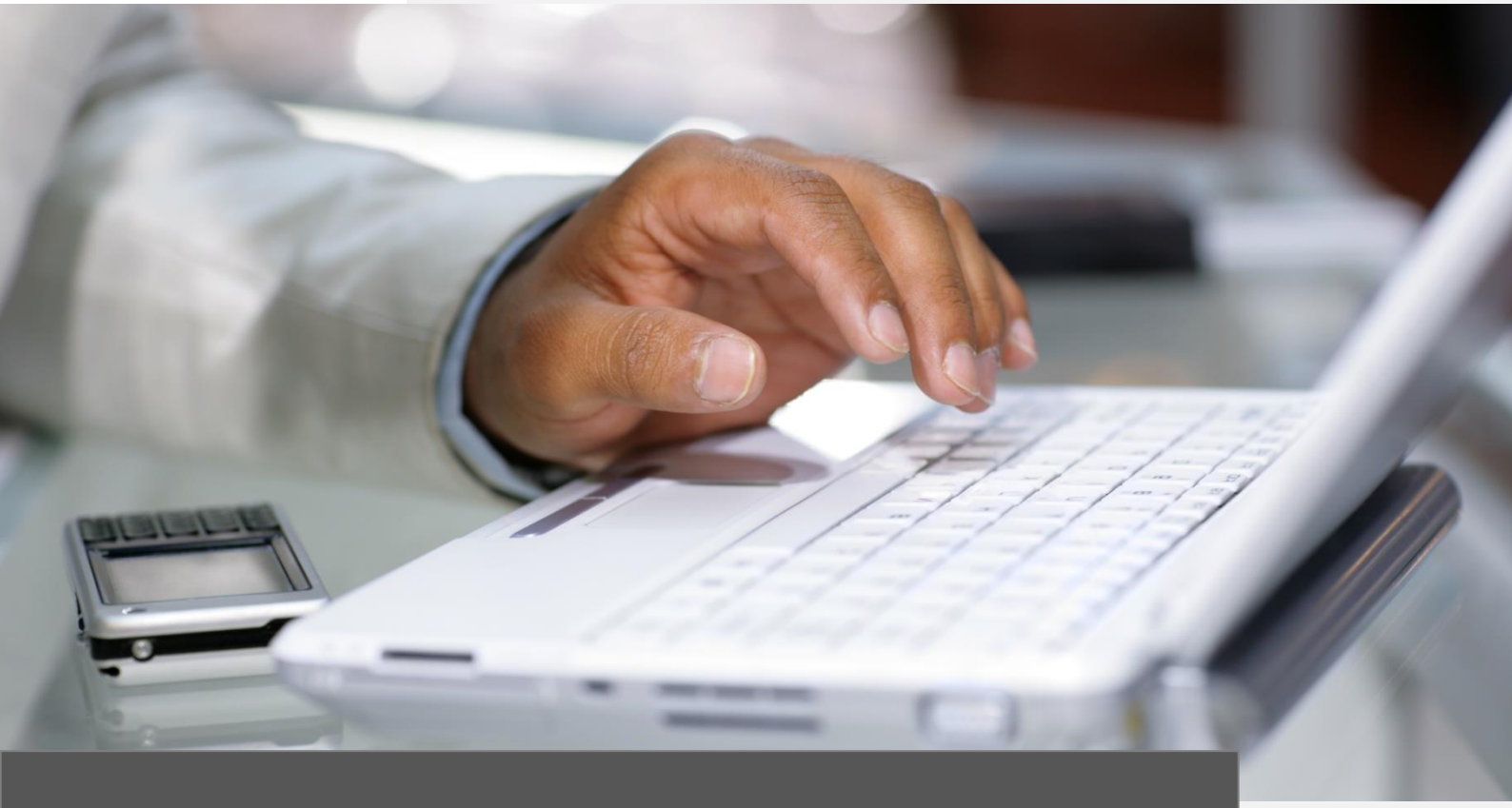
Die Datenschutzaufsichtsbehörden Baden-Württembergs, Bayerns, Hessens und des Saarlands stellen klar, dass auch sie „*bei Microsoft Office 365 erhebliche datenschutzrechtliche Verbesserungspotenziale*“ sehen, gerade auch mit Blick auf die jüngste Entscheidung des Europäischen Gerichtshofs zu internationalen Datentransfers vom 16. Juli 2020 (C-311/18 – Schrems II). Sie unterstützen deshalb im Grundsatz die Zielsetzungen des Arbeitskreises, soweit er Ansatzpunkte für datenschutzrechtliche Verbesserungen des Produkts Microsoft Office 365 formuliert. Seine Gesamtbewertung können sie allerdings schon deshalb nicht teilen, weil sie zu undifferenziert ausfällt. Überdies hat der Arbeitskreis Verwaltung seine Bewertung auf der Grundlage von Vertragsbestimmungen getroffen, die Microsoft zwischenzeitlich zweimal überarbeitet hat. Zudem konnten die Feststellungen des EuGH zu den Anforderungen der Datenschutz-Grundverordnung an internationale Datentransfers noch nicht berücksichtigt werden.

*Dies hat zur Folge, dass der Einsatz von Microsoft 365, und auch von vielen weiteren Clouddiensten, weiterhin von jedem Unternehmen kritisch hinterfragt und datenschutzrechtliche Entscheidungen immer gut dokumentiert werden sollten.*

Quelle der Informationen:

02.10.2020: Pressemitteilung der Aufsichtsbehörden von Baden-Württemberg, Bayern, Hessen und Saarland

Oktober | 2020



# Impressum

**CTV GmbH & Co.KG**
**Dipl.-Ing Veit Günl**
**Gewerbering 22**
**08112 Wilkau-Haßlau**

Amtsgericht Chemnitz, HRA 8539
Ust-IdNr.: DE 311232873

Geschäftsführer: A. Fehervari, C. Günl



**Redaktion**
Veit Günl

**Bildnachweise**
Diese Unterlage wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, Fuchsstädter Weg 2, 97491 Aidhausen erstellt. Einige der dargestellten Bilder wurden von der ITKservice bei https://www.ccvision.de gekauft und lizensiert. Weitere stammen von https://pixabay.com/de/ einer Plattform für lizenzfreie Bilder.