

24.  
MÄRZ

Digital arbeiten -  
jetzt erst recht!

26.  
MÄRZ

Corona-Virus und  
Arbeitsrecht:  
Fragen & Antworten

31.  
MÄRZ

Corona-Virus und  
Datenschutz:  
Was Unternehmen  
beachten müssen.

Weitere Informationen finden Sie unter: <https://www.wir-rv.de/corona>



# Corona-Virus

und Datenschutz

RA und FA IT-Recht **Stefan Lutz**, LL.M.  
IT-Kanzlei Lutz, Ravensburg

# Agenda

## 01 DSGVO Kurz und Knackig

Kurzer Überblick über die relevanten Erlaubnistatbestände zur Datenverarbeitung in der Krise

## 02 Datenverarbeitungen

Welche Daten darf ich erheben? Welche Probleme kommen hier auf mich zu? Beschäftigtendaten und Besucher.

## 03 Home Office

Messenger, Videokonferenztools & Co. Welche datenschutzrechtlichen Anforderungen bestehen? TOMs im Home Office. Datensicherheit in Corona Zeiten

## 04 Fragen über Fragen

Und ganz viele Antworten



# 01 DSGVO



# 01 DSGVO

## Brot und Butter Norm: Art. 5 DSGVO

Personenbezogene Daten müssen

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**“);
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („**Zweckbindung**“);
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („**Datenminimierung**“);

# 01 DSGVO

## Brot und Butter Norm: Art. 5 DSGVO

Personenbezogene Daten müssen

- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („**Richtigkeit**“);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („**Speicherbegrenzung**“);

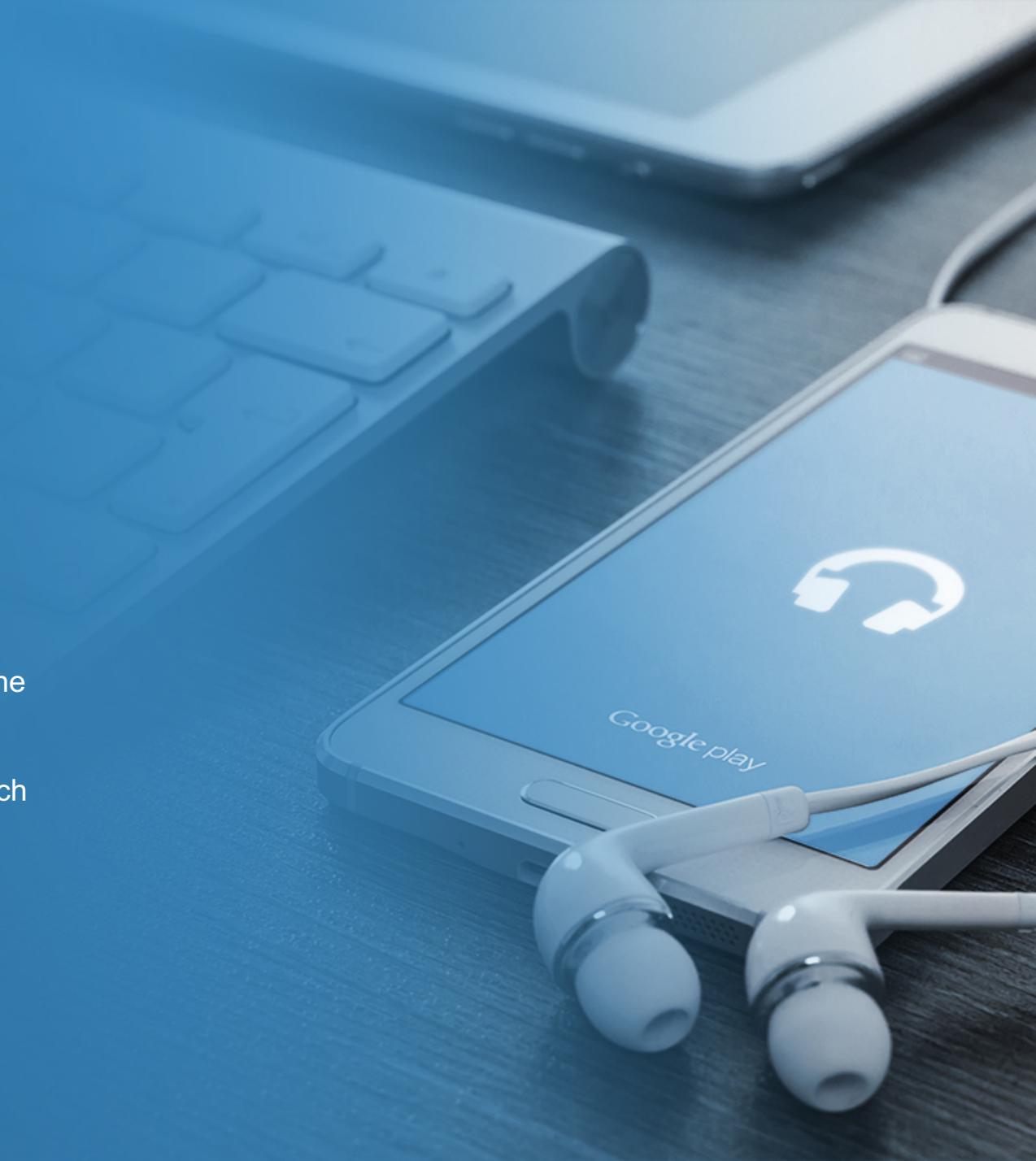
# 01 DSGVO

## Brot und Butter Norm: Art. 5 DSGVO

Personenbezogene Daten müssen

- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität und Vertraulichkeit**“);

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („**Rechenschaftspflicht**“).



# 01 DSGVO

## Erlaubnistatbestände Art. 6 DSGVO

<sup>1</sup>Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- b) die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- c) die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;
- d) die Verarbeitung ist erforderlich, um **lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen**;

# 01 DSGVO

## Erlaubnistatbestände Art. 6 DSGVO

<sup>1</sup>Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

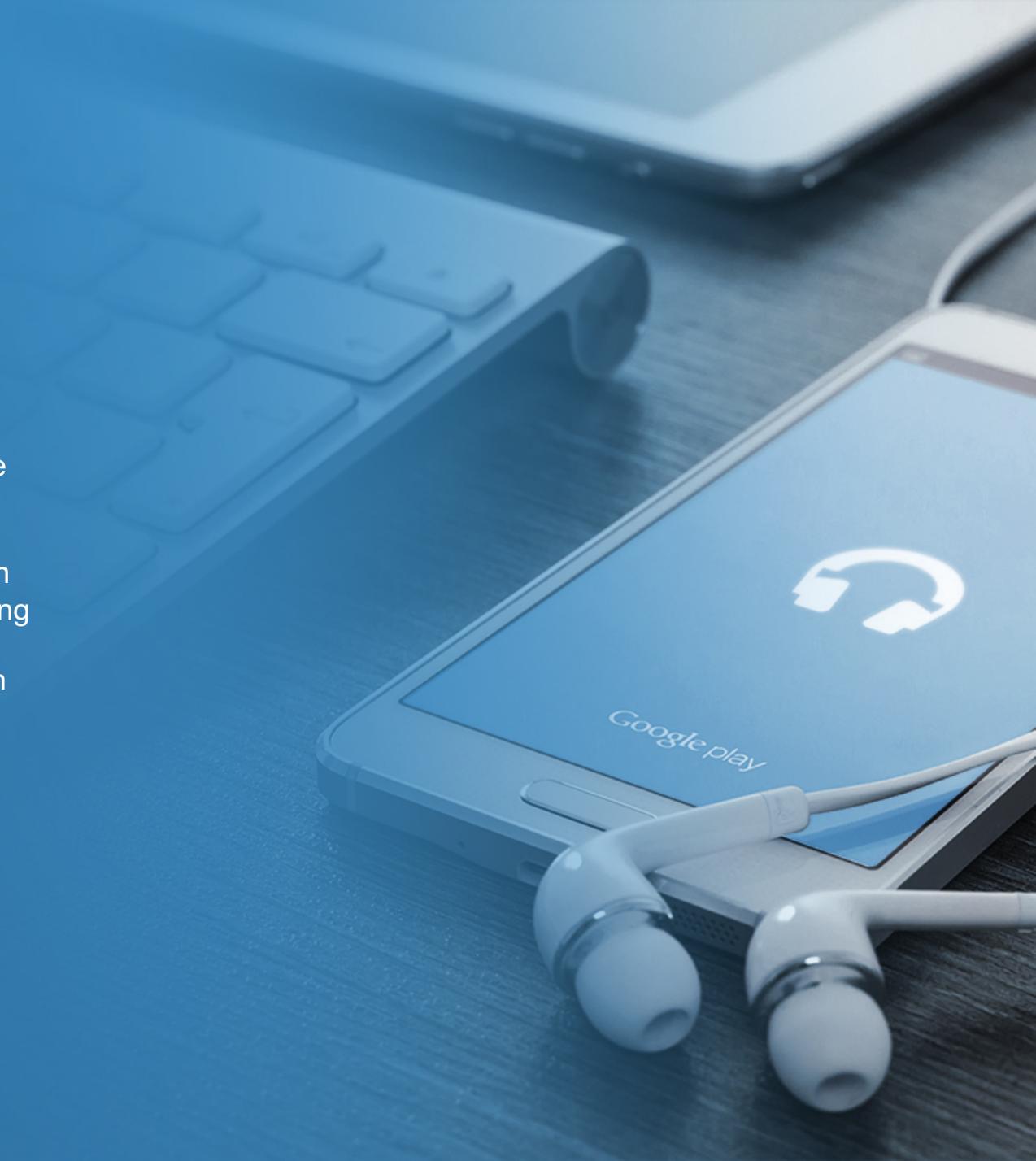
- e) die Verarbeitung ist für die **Wahrnehmung einer Aufgabe** erforderlich, die im **öffentlichen Interesse** liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- f) die Verarbeitung ist zur **Wahrung der berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.



# 01 DSGVO

## Gesundheitsbezogene Daten Art. 9 DSGVO

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person **ist untersagt.**

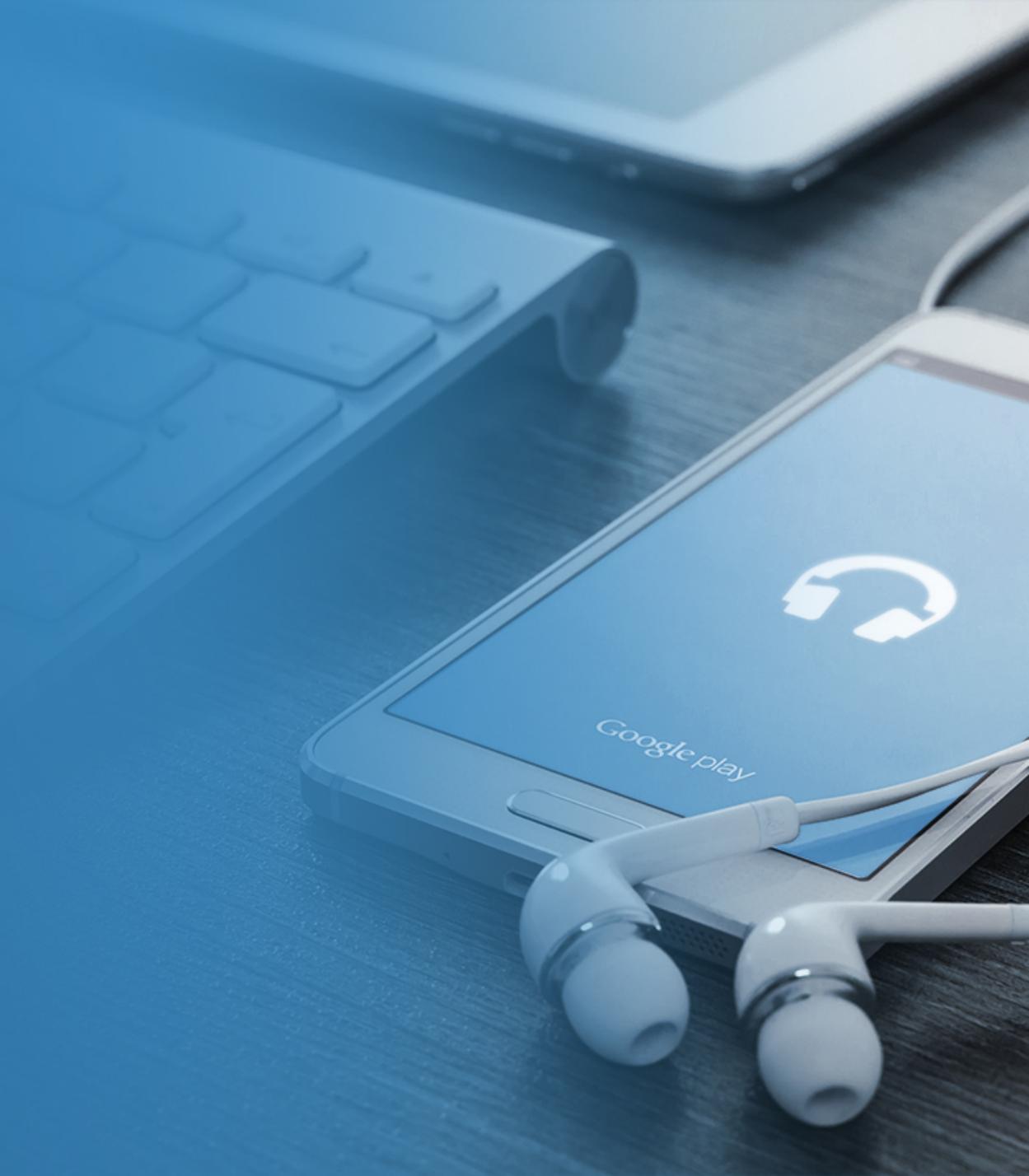


# 01 DSGVO

## Gesundheitsbezogene Daten Art. 9 DSGVO

Absatz 1 gilt nicht in folgenden Fällen:

- a. Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,
- b. die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,



# 01 DSGVO

## Gesundheitsbezogene Daten Art. 9 DSGVO

Absatz 1 gilt nicht in folgenden Fällen:

- c. die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,



A man with a beard and glasses, wearing a dark suit and tie, is sitting at a table. He is looking down at a smartphone in his hands. To his right, there is a glass mug with a spoon. The background is a solid blue color.

## 02 Datenverarbeitungen

# 02 Datenverarbeitungen

## Beschäftigtendatenschutz; § 26 BDSG

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über **die Begründung** eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für **dessen Durchführung** oder **Beendigung** oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. <sup>2</sup>Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.



# 02 Datenverarbeitungen

Beschäftigtendatenschutz; § 26 Abs. 3 BDSG

Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, **wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.** <sup>2</sup>Absatz 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. <sup>3</sup>§ 22 Absatz 2 gilt entsprechend.



# 02 Datenverarbeitungen

## Gesundheitsdaten; § 22 BDSG

Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig durch öffentliche und nichtöffentliche Stellen, wenn sie

- a. erforderlich ist, um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen,
- b. zum **Zweck der Gesundheitsvorsorge**, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden,



# 02 Datenverarbeitungen

## Gesundheitsdaten; § 22 BDSG

Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig durch öffentliche und nichtöffentliche Stellen, wenn sie

- c. aus **Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren** oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist; ergänzend zu den in Absatz 2 genannten Maßnahmen sind insbesondere die berufrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten, oder
- d. aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist,



# 02 Datenverarbeitungen

Gesundheitsdaten; § 22 Abs. 3 BDSG

In den Fällen des Absatzes 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. **<sup>2</sup>Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:**



# 02 Datenverarbeitungen

Gesundheitsdaten; § 22 Abs. 3 BDSG TOMs

1. **technisch organisatorische Maßnahmen**, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,
2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, **ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind**,
3. **Sensibilisierung** der an Verarbeitungsvorgängen Beteiligten,
4. **Benennung einer oder eines Datenschutzbeauftragten**,
5. **Beschränkung des Zugangs** zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
6. **Pseudonymisierung** personenbezogener Daten,
7. **Verschlüsselung** personenbezogener Daten,

# 02 Datenverarbeitungen

Gesundheitsdaten; § 22 Abs. 3 BDSG TOMs

8. Sicherstellung der Fähigkeit, **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
9. zur Gewährleistung der Sicherheit der Verarbeitung die **Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit** der technischen und organisatorischen Maßnahmen oder
10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.



# 03 Home Office



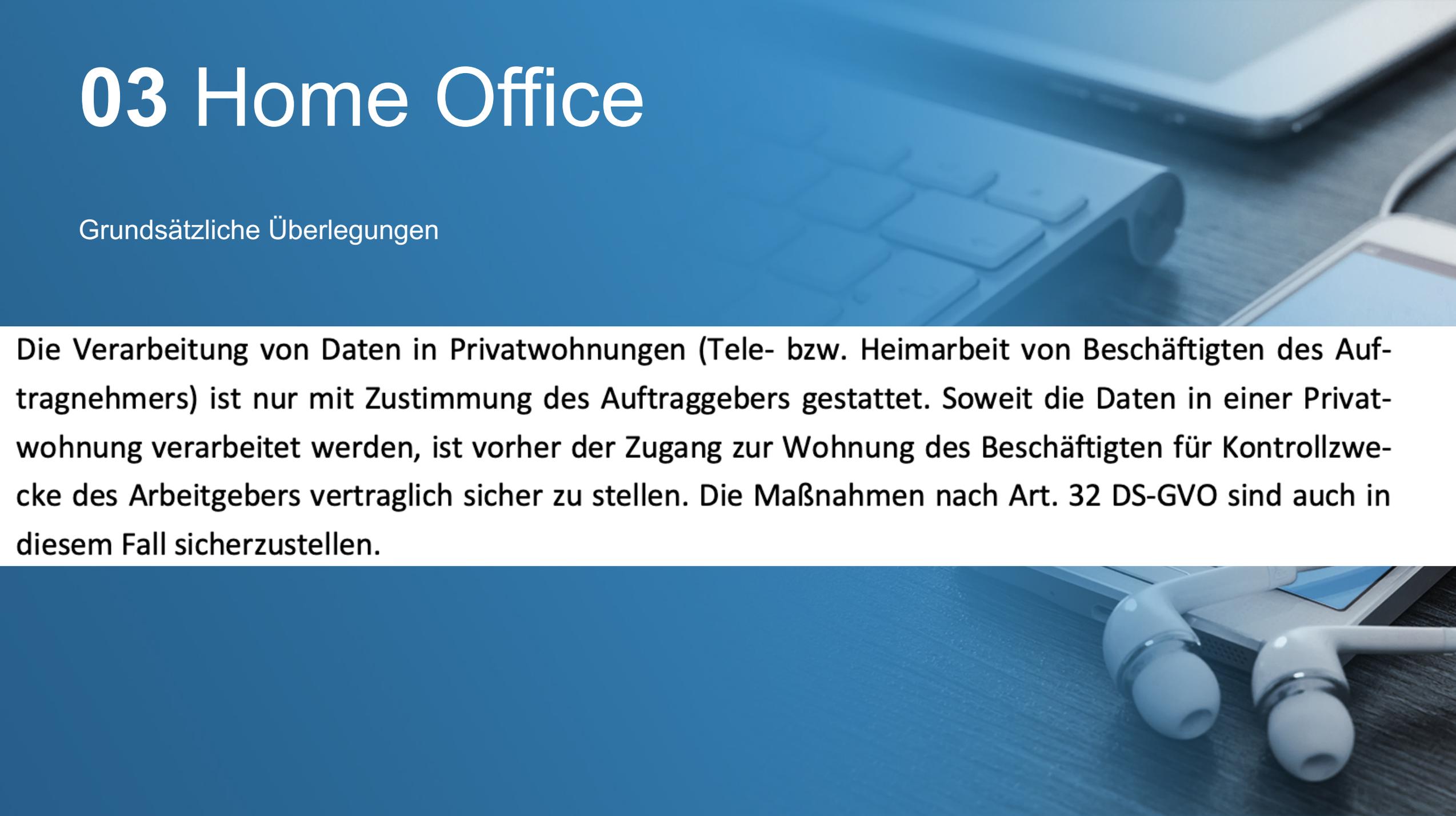
# 03 Home Office

## Grundsätzliche Überlegungen

- Ist die Arbeit grundsätzlich geeignet für Home Office?
  - Z.B. ungeeignet Call Center oder Bestellannahme
  - Geeignet: Allgemeine Bürotätigkeiten
- Technische und Organisatorische Maßnahmen ergreifen
- Home Office Vereinbarungen schließen
- **Vorsicht:** Möglicherweise in Auftragsverarbeitungsverträgen **verboten!**



# 03 Home Office



## Grundsätzliche Überlegungen

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

# 03 Home Office

## Videokonferenzsysteme – Aufsichtsbehörde

Bei der Auswahl von Video- oder Telefonkonferenzsystemen sollte aus technischer Sicht darauf geachtet werden, dass der Anbieter weder Metadaten (wer hat wann mit wem kommuniziert) noch die Inhaltsdaten der Kommunikation für eigene Zwecke auswertet oder an Dritte weitergibt. Dies können datenschutzrechtlich Verantwortliche am besten sicherstellen, wenn sie oder ihr Dienstleister (im öffentlichen Bereich sind das z.B. BITBW bei Landesbehörden oder ITEOS bei Kommunen) eine entsprechende Softwarelösung „On-Premises“ – also im eigenen Rechenzentrum – bereitstellen oder aufbauen. Dadurch ist es möglich, alle Datenflüsse und Datenerhebungen selbst zu kontrollieren. Dazu bieten sich zahlreiche Lösungen auf Basis von Open-Source-Software an (z.B. Nextcloud Talk, Jitsi Meet, RocketChat oder Matrix), die prinzipiell datenschutzgerecht einsetzbar sind.

### Details

Bei der Verarbeitung personenbezogener Daten haben Verantwortliche die allgemeinen Anforderungen der DS-GVO einzuhalten. Insbesondere ist bei der Auswahl von Kommunikationslösungen im speziellen darauf zu achten, dass die Verantwortlichkeit, ggf. gemeinsame Verantwortlichkeit, geklärt ist und nötige Verträge geschlossen werden, Datenverarbeitung (auch von Analyse-, Telemetrie- und Diagnosedaten) nur aufgrund und im Rahmen einer Rechtsgrundlage stattfindet, die Datenverarbeitung fair und transparent ist und Übermittlungen in das Ausland außerhalb des EWR nur unter den besonderen einschlägigen Voraussetzungen stattfindet.

Hierzu sollten sich Verantwortliche vorab einen Überblick über Vertragsverhältnisse und Datenflüsse (Zwecke, übertragene Daten, Empfänger) verschaffen.

Häufig sind Anwendungen datenschutzfreundlicher, die selbst betrieben werden können („On Premises“), beispielsweise auf eigenen Servern oder mit Hilfe von Dienstleistern mit Auftragsverarbeitungsverträgen. Der Vorteil ist, dass dort personenbezogene Daten wie Metadaten (wer hat wann mit wem kommuniziert) oder Inhaltsdaten der Kommunikation (z.B. Videobild, Screensharing) grundsätzlich nicht an Dritte übertragen werden. Zu den möglichen selbst betriebenen, von uns nicht im Detail geprüften, Lösungen aus verschiedenen Bereichen zählen beispielsweise:

- Nextcloud Talk: <https://nextcloud.com/talk/>
- Jitsi Meet: <https://jitsi.org/jitsi-meet/>
- RocketChat: <https://rocket.chat/>
- Matrix: <https://matrix.org/>



# 03 Home Office

## Videokonferenzsysteme – Beispiel Zoom

Datenschutzkonforme Lösung möglich

1. Auftragsverarbeitungsvertrag schließen
2. Informationspflichten nach Art. 13 DSGVO bereithalten
3. Achtung Berufsgeheimnisträger: Einwilligungen einholen

<https://www.datenschutz-guru.de/datenschutz-tipps-6-2020-muster-anleitungen-co-fuer-online-meetings-via-zoom/>



# 03 Home Office

Videokonferenzsysteme – Beispiel Zoom

**Datenschutzhinweise für Online-Meetings, Telefonkonferenzen und Webinare via „Zoom“ der Mustermann GmbH**

Wir möchten Sie nachfolgend über die Verarbeitung personenbezogener Daten im Zusammenhang mit der Nutzung von „Zoom“ informieren.

## Zweck der Verarbeitung

Wir nutzen das Tool „Zoom“, um Telefonkonferenzen, Online-Meetings, Videokonferenzen und/oder Webinare durchzuführen (nachfolgend: „Online-Meetings“). „Zoom“ ist ein Service der Zoom Video Communications, Inc., die ihren Sitz in den USA hat.



# 03 Home Office

## Videokonferenzsysteme – Beispiel Zoom

### Verantwortlicher

**Verantwortlicher** für Datenverarbeitung, die im unmittelbaren Zusammenhang mit der Durchführung von „Online-Meetings“ steht, ist die Mustermann GmbH.

**Hinweis:** Soweit Sie die Internetseite von „Zoom“ aufrufen, ist der Anbieter von „Zoom“ für die Datenverarbeitung verantwortlich. Ein Aufruf der Internetseite ist für die Nutzung von „Zoom“ jedoch nur erforderlich, um sich die Software für die Nutzung von „Zoom“ herunterzuladen.

Sie können „Zoom“ auch nutzen, wenn Sie die jeweilige Meeting-ID und ggf. weitere Zugangsdaten zum Meeting direkt in der „Zoom“-App eingeben.

Wenn Sie die „Zoom“-App nicht nutzen wollen oder können, dann sind die Basisfunktionen auch über eine Browser-Version nutzbar, die Sie ebenfalls auf der Website von „Zoom“ finden.

# 03 Home Office

## Videokonferenzsysteme – Beispiel Zoom

### Welche Daten werden verarbeitet?

Bei der Nutzung von „Zoom“ werden verschiedene Datenarten verarbeitet. Der Umfang der Daten hängt dabei auch davon ab, welche Daten Sie vor bzw. bei der Teilnahme an einem „Online-Meeting“ machen.

Folgende personenbezogene Daten sind Gegenstand der Verarbeitung:

**Angaben zum Benutzer:** Vorname, Nachname, Telefon (optional), E-Mail-Adresse, Passwort (wenn „Single-Sign-On“ nicht verwendet wird), Profilbild (optional), Abteilung (optional)

**Meeting-Metadaten:** Thema, Beschreibung (optional), Teilnehmer-IP-Adressen, Geräte-/Hardware-Informationen

# 03 Home Office

## Videokonferenzsysteme – Beispiel Zoom

**Bei Aufzeichnungen (optional):** MP4-Datei aller Video-, Audio- und Präsentationsaufnahmen, M4A-Datei aller Audioaufnahmen, Textdatei des Online-Meeting-Chats.

**Bei Einwahl mit dem Telefon:** Angabe zur eingehenden und ausgehenden Rufnummer, Ländername, Start- und Endzeit. Ggf. können weitere Verbindungsdaten wie z.B. die IP-Adresse des Geräts gespeichert werden.

**Text-, Audio- und Videodaten:** Sie haben ggf. die Möglichkeit, in einem „Online-Meeting“ die Chat-, Fragen- oder Umfragenfunktionen zu nutzen. Insoweit werden die von Ihnen gemachten Texteingaben verarbeitet, um diese im „Online-Meeting“ anzuzeigen und ggf. zu protokollieren. Um die Anzeige von Video und die Wiedergabe von Audio zu ermöglichen, werden entsprechend während der Dauer des Meetings die Daten vom Mikrophon Ihres Endgeräts sowie von einer etwaigen Videokamera des Endgeräts verarbeitet. Sie können die Kamera oder das Mikrophon jederzeit selbst über die „Zoom“-Applikationen abschalten bzw. stummstellen.

Um an einem „Online-Meeting“ teilzunehmen bzw. den „Meeting-Raum“ zu betreten, müssen Sie zumindest Angaben zu Ihrem Namen machen.

# 03 Home Office

## Videokonferenzsysteme – Beispiel Zoom

### Umfang der Verarbeitung

Wir verwenden „Zoom“, um „Online-Meetings“ durchzuführen. Wenn wir „Online-Meetings“ aufzeichnen wollen, werden wir Ihnen das im Vorwege transparent mitteilen und – soweit erforderlich – um eine Zustimmung bitten. Die Tatsache der Aufzeichnung wird Ihnen zudem in der „Zoom“-App angezeigt.

Wenn es für die Zwecke der Protokollierung von Ergebnissen eines Online-Meetings erforderlich ist, werden wir die Chatinhalte protokollieren. Das wird jedoch in der Regel nicht der Fall sein.

Im Falle von Webinaren können wir für Zwecke der Aufzeichnung und Nachbereitung von Webinaren auch die gestellten Fragen von Webinar-Teilnehmenden verarbeiten.

Wenn Sie bei „Zoom“ als Benutzer registriert sind, dann können Berichte über „Online-Meetings“ (Meeting-Metadaten, Daten zur Telefoneinwahl, Fragen und Antworten in Webinaren, Umfragefunktion in Webinaren) bis zu einem Monat bei „Zoom“ gespeichert werden.

Die in „Online-Meeting“-Tools wie „Zoom“ bestehende Möglichkeit einer softwareseitigen „Aufmerksamkeitsüberwachung“ („Aufmerksamkeitstracking“) ist **deaktiviert**.

Eine automatisierte Entscheidungsfindung i.S.d. Art. 22 DSGVO kommt nicht zum Einsatz.

# 03 Home Office

## Videokonferenzsysteme – Beispiel Zoom

### Rechtsgrundlagen der Datenverarbeitung

Soweit personenbezogene Daten von Beschäftigten der Mustermann GmbH verarbeitet werden, ist § 26 BDSG die Rechtsgrundlage der Datenverarbeitung. Sollten im Zusammenhang mit der Nutzung von „Zoom“ personenbezogene Daten nicht für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich, gleichwohl aber elementarer Bestandteil bei der Nutzung von „Zoom“ sein, so ist Art. 6 Abs. 1 lit. f) DSGVO die Rechtsgrundlage für die Datenverarbeitung. Unser Interesse besteht in diesen Fällen an der effektiven Durchführung von „Online-Meetings“.

Im Übrigen ist die Rechtsgrundlage für die Datenverarbeitung bei der Durchführung von „Online-Meetings“ Art. 6 Abs. 1 lit. b) DSGVO, soweit die Meetings im Rahmen von Vertragsbeziehungen durchgeführt werden.

Sollte keine vertragliche Beziehung bestehen, ist die Rechtsgrundlage Art. 6 Abs. 1 lit. f) DSGVO. Auch hier besteht unser Interesse an der effektiven Durchführung von „Online-Meetings“.



# 03 Home Office

## Videokonferenzsysteme – Beispiel Zoom

### Empfänger / Weitergabe von Daten

Personenbezogene Daten, die im Zusammenhang mit der Teilnahme an „Online-Meetings“ verarbeitet werden, werden grundsätzlich nicht an Dritte weitergegeben, sofern sie nicht gerade zur Weitergabe bestimmt sind. Beachten Sie bitte, dass Inhalte aus „Online-Meetings“ wie auch bei persönlichen Besprechungstreffen häufig gerade dazu dienen, um Informationen mit Kunden, Interessenten oder Dritten zu kommunizieren und damit zur Weitergabe bestimmt sind.

Weitere Empfänger: Der Anbieter von „Zoom“ erhält notwendigerweise Kenntnis von den o.g. Daten, soweit dies im Rahmen unseres Auftragsverarbeitungsvertrages mit „Zoom“ vorgesehen ist.

# 03 Home Office

## Videokonferenzsysteme – Beispiel Zoom

### Datenverarbeitung außerhalb der Europäischen Union

„Zoom“ ist ein Dienst, der von einem Anbieter aus den USA erbracht wird. Eine Verarbeitung der personenbezogenen Daten findet damit auch in einem Drittland statt. Wir haben mit dem Anbieter von „Zoom“ einen Auftragsverarbeitungsvertrag geschlossen, der den Anforderungen von Art. 28 DSGVO entspricht.

Ein angemessenes Datenschutzniveau ist zum einen durch die „Privacy Shield“-Zertifizierung der Zoom Video Communications, Inc., zum anderen aber auch durch den Abschluss der sog. EU-Standardvertragsklauseln garantiert.

### Datenschutzbeauftragter

Wir haben einen Datenschutzbeauftragten benannt.

Sie erreichen diesen wie folgt: Mustermann GmbH, - Datenschutzbeauftragte/r –, Musterstr. 123, 12345 Musterstadt, E-Mail: [datenschutz@mustermann.de](mailto:datenschutz@mustermann.de)

# 03 Home Office

## Videokonferenzsysteme – Beispiel Zoom

### Ihre Rechte als Betroffene/r

Sie haben das Recht auf **Auskunft** über die Sie betreffenden personenbezogenen Daten. Sie können sich für eine Auskunft jederzeit an uns wenden.

Bei einer Auskunftsanfrage, die nicht schriftlich erfolgt, bitten wir um Verständnis dafür, dass wir ggf. Nachweise von Ihnen verlangen, die belegen, dass Sie die Person sind, für die Sie sich ausgeben.

Ferner haben Sie ein Recht auf **Berichtigung** oder **Löschung** oder auf **Einschränkung** der Verarbeitung, soweit Ihnen dies gesetzlich zusteht.

Schließlich haben Sie ein **Widerspruchsrecht** gegen die Verarbeitung im Rahmen der gesetzlichen Vorgaben.

Ein Recht auf **Datenübertragbarkeit** besteht ebenfalls im Rahmen der datenschutzrechtlichen Vorgaben.

# 03 Home Office

## Videokonferenzsysteme – Beispiel Zoom

### Löschung von Daten

Wir löschen personenbezogene Daten grundsätzlich dann, wenn kein Erfordernis für eine weitere Speicherung besteht. Ein Erfordernis kann insbesondere dann bestehen, wenn die Daten noch benötigt werden, um vertragliche Leistungen zu erfüllen, Gewährleistungs- und ggf. Garantieansprüche prüfen und gewähren oder abwehren zu können. Im Falle von gesetzlichen Aufbewahrungspflichten kommt eine Löschung erst nach Ablauf der jeweiligen Aufbewahrungspflicht in Betracht.

### Beschwerderecht bei einer Aufsichtsbehörde

Sie haben das Recht, sich über die Verarbeitung personenbezogener Daten durch uns bei einer **Aufsichtsbehörde** für den Datenschutz zu beschweren.



# 03 Home Office

## Videokonferenzsysteme – MS Teams?

### Was die Gratis-Version kann – und was nicht

In der kostenlosen Variante von Microsoft Teams können Anwender insgesamt bis zu 300 Personen pro Unternehmen in Chatgruppen einladen. Funktionen wie etwa Terminvereinbarungen für Anrufe oder Audio- und Videokonferenzen sind hingegen erst mit Office 365 verfügbar, das Microsoft Teams mit Vollintegration in die Office-Anwendungen beinhaltet. Damit stehen Nutzern auch weitere Dienste für die effiziente Zusammenarbeit zur Verfügung wie der Online-Speicher OneDrive, SharePoint und Yammer. Die Vollversion bietet dann auch eine Integration der vorhandenen Telefonanlage mittels Direct Routing an, setzt dabei aber einen der Enterprise-Kostenpläne von Office 365 voraus. Auch beim Speicherplatz zieht Microsoft eine Grenze: Dieser ist bei der kostenlosen Version auf zwei GB pro Benutzer beschränkt, zehn GB Speicher erhält jedes Team obendrauf. Die Nutzer der kostenpflichtigen Varianten erhalten deutlich größere Kapazitäten von einem Terabyte pro User.



# 03 Home Office

## Videokonferenzsysteme – MS Teams?

### Datensicherheit in der Cloud

Microsoft bietet alle Versionen aus sicheren EU-Rechenzentren und Unternehmen damit Datenverarbeitung gemäß der Anforderungen aus der EU-DSGVO an; alle Daten werden dabei verschlüsselt übertragen und gespeichert. Unternehmen, die über die Kommunikationsplattform sensible, datenschutzrelevante Informationen austauschen wollen, sollten sich für eine der kostenpflichtigen Versionen entscheiden, die mit Zugriff auf das Security & Compliance Center eine Anzahl an Sicherheits-Features mit sich bringen: So können sie beispielsweise eine mehrstufige Authentifizierung (Multi-Factor Authentication, MFA) für Benutzeranmeldungen nutzen. Neben dem obligatorischen Kennwort bietet diese MFA eine zusätzliche, nutzerspezifische Sicherheitsebene, die Unternehmen individuell konfigurieren können. Der Mitarbeiter muss sich dann je nach zugewiesener Richtlinie etwa über ein bestimmtes Smartphone oder per Fingerabdruck identifizieren.

# 03 Home Office

## Videokonferenzsysteme – MS Teams?

- Auch hier gilt:
- AVV schließen – sofern MS dies zulässt (möglicherweise auch Joint Controllership)
- DPA (Data Processing Agreement von MS wurde angepasst)
- Informationspflichten beachten
- Problem: Office365 wird derzeit von den Aufsichtsbehörden als **nicht** datenschutzkonform betrachtet!



# 03 Home Office

## Whatsapp & Co

<https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/>

### Fazit:

WhatsApp als Messenger-Dienst ist nicht a priori datenschutzwidrig, aktuelle Probleme resultieren weniger aus der Gestaltung des Dienstes, sondern aus dessen Einsatzbedingungen in der Praxis. Unabhängig von weiter bestehenden Bedenken hinsichtlich des Privacy Shields ist ein datenschutzkonformer WhatsApp-Einsatz unter bestimmten **Voraussetzungen** möglich. Hierzu zählen

- der Einsatz aktueller Software-Versionen, um eine Verschlüsselung der Kommunikationsinhalte zu gewährleisten
- der Einsatz dienstlicher/geschäftlicher Mobiltelefone; eine Nutzung privater Endgeräte kommt nur ausnahmsweise und verbunden mit tragfähigen Container-Lösungen in Betracht
- die Nutzung eines „one-record-Adressbuchs“ mit ausschließlich der Telefonnummer des Diensteanbieters, eines Telefonbuchs mit ausschließlich WhatsApp-Kontakten oder eine Sperre des Adressbuchzugriffs durch WhatsApp
- die Deaktivierung von Cloud-Backups
- die Sicherstellung, dass Chat-Anhänge nicht in der Mediathek des Mobiltelefons gespeichert werden bzw. Dritt-Applikationen keine Zugriff darauf haben
- eine ausreichende Absicherung der Endgeräte (Zugriffssperre, Verschlüsselung)



# 03 Home Office

## Whatsapp & Co



# 03 Home Office

## Muster für eine Einwilligung für Beratung mittels WhatsApp

### WhatsApp Dienstbeschreibung

#### Dienstleister

WhatsApp ist Teil des Unternehmens Facebook und [arbeitet mit diesem zusammen](#).

Bei der Nutzung von WhatsApp erlauben Sie eine umfangreiche Verarbeitung Ihrer Daten einschließlich einer umfassenden Werbeeinwilligung zu Gunsten der Unternehmensgruppe.

#### Leistungen in Europa

Wenn Sie über WhatsApp mit uns in Kontakt treten, werden Ihre Daten auch von WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland verarbeitet im Rahmen eines Vertrages und einer Werbeeinwilligung mit dem Anbieter.

Dies gilt für die Staaten Andorra, Österreich, Azoren, Belgien, Bulgarien, Kanarische Inseln, Kanalinseln, Dänemark, Deutschland, Estland, Finnland, Frankreich, Französisch-Guayana, Griechenland, Guadeloupe, Island, Irland, Isle of Man, Italien, Lettland, Liechtenstein, Litauen, Luxemburg, Madeira, Malta, Tschechische Republik, Ungarn, Martinique, Mayotte, Monaco, Niederlande, Norwegen, Polen, Portugal, Republik Zypern, Réunion, Rumänien, San Marino, Saint Barthélemy, Saint-Martin, Slowakei, Slowenien, Spanien, Schweden, Schweiz, Großbritannien, souveräne britische Stützpunkte in Zypern (Akrotiri und Dekelia) und Vatikanstadt.

Dabei gelten die [Nutzungsbedingungen](#) und die [Datenschutzrichtlinie](#) von WhatsApp.

#### Leistungen außerhalb von Europa

Leben Sie nicht in den oben genannten Ländern werden die Leistungen von WhatsApp Inc., 1601 Willow Road, Menlo Park, Kalifornien 94025, Vereinigte Staaten von Amerika angeboten.

Ein rechtlich angemessenes Datenschutzniveau für die Datenübermittlung in die Vereinigte Staaten von Amerika ist für den Anbieter durch seine [EU-U.S. Privacy Shield Zertifizierung](#) garantiert.

Es finden auch die folgenden [Nutzungsbedingungen](#) und [Datenschutzrichtlinien](#) von WhatsApp Anwendung.

#### Risiken

Sie treten mit uns über einen Unternehmensaccount in Kontakt. Dadurch wird für WhatsApp und das Facebook-Unternehmen die Beziehung von Ihnen zu uns offengelegt und somit Ihr Profil unter anderem für zielgerichtete Werbung verbessert.

Dieses Element Ihres Profils kann nach unserer Erkenntnis nur durch ein Löschen der Profils einknüpft werden. Möglicherweise könnte diese Verknüpfung auch mit einem neu angelegten Profil fortbestehen, wenn Sie Ihre Kontakte zum gelöschten Profil nur unwesentlich unterscheiden oder sich Ihr Bewegungsprofil nicht ändert.

#### Einwilligung

Wenn Sie in Kenntnis dieser Risiken mit uns über den Dienst WhatsApp der WhatsApp Inc und WhatsApp Ireland Limited mit dem IT-Support in Kontakt treten möchten, klicken Sie unten auf die Schaltfläche.

Von Ihrer Einwilligung umfasst sind ferner Messungen und Analysen die wir Kommunikation mit Ihnen von WhatsApp erhalten.

**Sie können Ihre Einwilligung uns gegenüber jederzeit für die Zukunft mittels WhatsAppnachricht oder Mitteilung ans uns widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird.**

#### Information zur Datenverarbeitung

Diese stellen wir in unserer Datenschutzerklärung bereit.

# 03 Home Office

## ▼ Muster für eine Datenschutzerklärung

Als Stabsstelle möchte ich Ihnen ein unverbindliches Muster für die Datenschutzerklärung gemäß Art. 13 DSGVO zur Verfügung stellen.

### Verantwortlicher

...

### Datenschutzbeauftragter

...

### Betroffenenrechte

#### Allgemeine Rechte

Nach der Datenschutz-Grundverordnung stehen Ihnen folgende Rechte zu:

Werden Ihre personenbezogenen Daten verarbeitet, so haben Sie das Recht, Auskunft über die zu Ihrer Person gespeicherten Daten zu erhalten (Art. 15 DSGVO).

Sollten unrichtige personenbezogene Daten verarbeitet werden, steht Ihnen ein Recht auf Berichtigung zu (Art. 16 DSGVO).

Liegen die gesetzlichen Voraussetzungen vor, so können Sie die Löschung oder Einschränkung der Verarbeitung verlangen sowie Widerspruch gegen die Verarbeitung einlegen (Art. 17, 18 und 21 DSGVO).

Wenn Sie in die Datenverarbeitung eingewilligt haben oder ein Vertrag zur Datenverarbeitung besteht und die Datenverarbeitung mithilfe automatisierter Verfahren durchgeführt wird, steht Ihnen gegebenenfalls ein Recht auf Datenübertragbarkeit zu (Art. 20 DSGVO).

Sollten Sie von Ihren oben genannten Rechten Gebrauch machen, prüft die öffentliche Stelle, ob die gesetzlichen Voraussetzungen hierfür erfüllt sind.

Weiterhin besteht ein Beschwerderecht beim Bayerischen Landesbeauftragten für den Datenschutz.

#### Widerrufsrecht

Sie können, da der Verarbeitung Ihrer Daten eine Einwilligung zu Grunde liegt, die Einwilligung jederzeit widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird.



# 03 Home Office

## Zwecke und Rechtsgrundlagen der Verarbeitung

Beantwortung von Nachrichten über die Sofort-Nachrichtenservices WhatsApp und Threema, auf Grundlage von Art. 6 Abs. 1 lit. a DSGVO.

## Offenlegung personenbezogener Daten

Für WhatsApp an WhatsApp Inc., 1601 Willow Road, Menlo Park, Kalifornien 94025, Vereinigte Staaten von Amerika und WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland

Für Threema an Threema GmbH, Churerstrasse 82, 8808 Pfäffikon SZ, Schweiz

## Garantien für den Internationalen Datentransfer

Für WhatsApp: [🔗 Anbieterzertifizierung unter dem EU-U.S. Privacy Shield](#)

Für Threema: [🔗 Angemessenheitsbeschluss der EU Kommission für die Schweizerische Eidgenossenschaft](#)

## Regellöschfristen

Var. 1: Nach Abschluss der Unterhaltung oder Widerruf der Einwilligung

Var. 2: Nach Widerruf der Einwilligung ansonsten Prüfung zum Jahresende, ob Speicherungen für Anschlussanfragen weiterhin notwendig.



# 03 Home Office

## Whatsapp & Co

### ▼ Lizenzrechtliches

WhatsApp sollte in der Version WhatsApp Business genutzt werden, da die klassische Version von Anbieter die Nutzung jenseits privater Zwecke untersagt werden kann.

Threema bietet mit Threema Education ein passenden Lizenzangebot an.

Die Anbieter Signal und Telegram wären zwar lizenzrechtlich für Hochschulen nutzbar, jedoch sind Sie als Verantwortliche für die Datenverarbeitung bzw. als Auftragsverarbeiter nicht greifbar, bzw. es kann kein angemessenes Datenschutzniveau garantiert werden.

<https://www.rz.uni-wuerzburg.de/dienste/it-recht/whatsapp/>

# 03 Home Office

## Dropbox & Co

- Nutzung nur datenschutzkonform möglich, wenn Daten verschlüsselt sind!
- Passwort über sicheren Kommunikationsweg mitteilen (z.B. Telefon, SMS)
- Besser: Verschlüsselung der Dropbox mit z.B. Boxcryptor



# 03 Home Office

## Was gilt es zu regeln?

- Sensibilisierung der Mitarbeiter
- Zutritts- und Zugriffsschutz
- Härtung der eingesetzten IT-Systeme
- Verschlüsselung der mobilen Endgeräte (auch Festplatten)
- Blickschutzfolien
- Einsatz von VPN
- Datensicherung bei mobilen Endgeräten
- Zeitnahe Verlustmeldung (72 Stundenfrist für Datenschutzpannen)
- Entsorgung von vertraulichen Informationen...

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompodium/umsetzungshinweise/OPS/Umsetzungshinweise\\_zum\\_Baustein\\_OPS\\_1\\_2\\_4\\_Telearbeit.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompodium/umsetzungshinweise/OPS/Umsetzungshinweise_zum_Baustein_OPS_1_2_4_Telearbeit.html)

<https://www.datenschutzzentrum.de/artikel/1322-Ploetzlich-im-Homeoffice-und-der-Datenschutz-Die-Landesbeauftragte-fuer-Datenschutz-Schleswig-Holstein-informiert.html>

<https://www.datenschutz-guru.de/corona-virus-richtlinie-zur-heimarbeit-home-office-zum-download/>



A man with a beard and glasses, wearing a dark suit and tie, is seated at a dark wooden table. He is looking down at a smartphone held in his hands. To his right, on the table, is a clear glass mug containing a beverage with a spoon. The background is a solid, deep blue color.

# 04 Fragen

# 04 Fragen

## Eingegangene Fragen

- Nutzung von Videokonferenz-Tools: Was ist zu beachten? Sind diese DSGVO konform? Wie sieht es z.B. mit ZOOM aus, deren Server in den USA steht?
- Was ist zu beachten, wenn man eine Aufzeichnung macht bei einer Konferenz, bei der auch persönliche Daten / Themen ausgetauscht werden, z.B. wie bei einem Workshop und anderen Teilnehmern dieser Gruppe (die z.B. nicht teilnehmen konnten) zur Verfügung stellt?



# 04 Fragen

## Eingegangene Fragen

- Viele Firmen nutzen Microsoft Teams. Ist das grds. DSGVO konform oder muss hier zusätzlich etwas beachtet werden, z.B. wenn MS Team mit Teilnehmern aus verschiedenen Firmen genutzt wird und auch persönliche Daten darüber ausgetauscht werden? Ist MS Teams free auch DSGVO konform?
- Daten/Dateien mit (kostenloser) Dropbox oder WeTransfer verschicken. Wie sicher und DSGVO konform ist das?
- Nutzung von WhatsApp mit Freigabe der eigenen Kontakte: Ist das datenschutzrechtlich erlaubt? Ich denke nicht, aber viele Firmen/Mitarbeiter machen das auch für berufliche Zwecke. Was sind die Risiken? Wie sieht es mit passiver WhatsApp Nutzung aus, bei der man seine Kontakte nicht freigibt? Wie sieht das datenschutzrechtlich aus?



A man with a beard and glasses, wearing a dark suit and a red tie, is sitting at a table. He is looking down at a smartphone in his hands. In the foreground, there is a glass mug with a spoon. The background is a solid blue color.

# 04 Weitere Fragen

Bitte nutzen Sie die “F&A Funktion”, um weitere Fragen zu stellen.



# Vielen Dank

RA und FA IT-Recht **Stefan Lutz**, LL.M.  
IT-Kanzlei Lutz  
Bachstr. 3  
88214 Ravensburg  
[www.datenschutz-rv.de](http://www.datenschutz-rv.de)