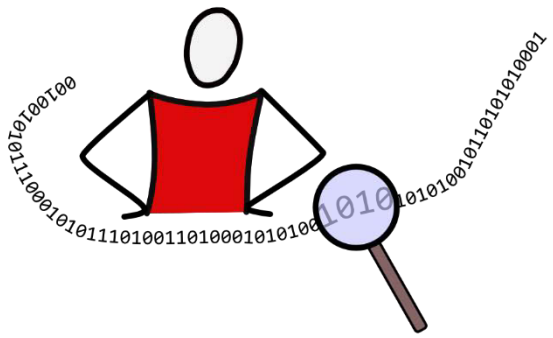
Datenschutz: Plötzlich Videokonferenzen – und nun?

Im Zuge der Corona-Pandemie hat sich vieles im Alltagsleben sehr schnell verändert. Dazu gehören auch das Arbeiten von zu Hause und die Kommunikation über Videokonferenzen. Falls Sie unvermittelt Videokonferenzen ausrichten oder an Videokonferenzen teilnehmen müssen, haben wir einige einfache Regeln und Hinweise für den Umgang mit personenbezogenen Daten, die Sie sofort umsetzen können.

Die erste und grundsätzliche Frage, die Sie sich stellen sollten, ist, ob eine Videokonferenz tatsächlich für die jeweilige Situation das richtige Mittel der Kommunikation ist. Einerseits gibt es den Vorteil, Gestik und Mimik der anderen Teilnehmenden sehen zu können, andererseits bestehen auch Risiken. Wenn eine Telefonkonferenz oder schriftliche Kommunikation ausreicht, kann man einige Risiken vermeiden.

Datenschutzprobleme identifizieren

Videokonferenzen kommen in sehr verschiedenen Situationen zum Einsatz, die wiederum unterschiedliche Anforderungen an den Datenschutz stellen, z. B. im Beruf, in Bildungseinrichtungen, in Ehrenämtern oder Vereinsaktivitäten oder in Familie und Freundeskreis. Eine Kurzbetrachtung von Einsatz-Szenarien und spezielle Hinweise finden Sie im Anhang.



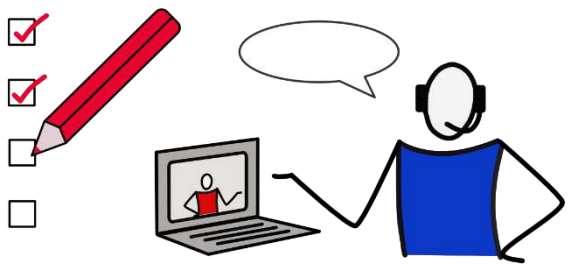
Mit der Übertragung von Bildern von Personen werden automatisch personenbezogene Daten übertragen – je nach Inhalt der Konferenz können noch sensiblere oder weitere Daten von Dritten hinzukommen. Im Folgenden finden Sie eine Reihe genereller Regeln und Hinweise. Sie richten sich im Wesentlichen an zwei Gruppen:

- **Organisierende Personen**, die eine Videokonferenz verwalten und einrichten: Sie können bereits in der Vorbereitung technische und organisatorische Maßnahmen berücksichtigen, die dem Datenschutz aller dienen.
- **Teilnehmende Personen** an einer Videokonferenz: Auch hier gilt es, einfache Regeln und Hinweise zu beachten, z. B. wenn über andere Personen gesprochen wird.

Für die **organisierenden Personen** einer Videokonferenz sind zunächst die Rahmenbedingungen zu klären. Im beruflichen Einsatz stehen manchmal andere Lösungen zur Verfügung als beispielsweise im ehrenamtlichen Verein, und ggf. muss man auch andere Vorgaben beachten. Ein Blick in die Einsatz-Szenarien im Anhang kann hilfreich sein, außerdem sollten übergeordnete Fragestellungen berücksichtigt werden wie z. B.:

- Wenn Sie Videokonferenzen **beruflich einsetzen müssen**, dann hat Ihr Unternehmen bzw. Ihre Behörde die Wahl zwischen einem Online-Dienst (SaaS, Software as a Service) oder eine Lösung, die auf den eigenen Servern und im eigenen Netzwerk installiert ist (On-Premises-Lösung).
  - Wird eine **Videokonferenzsoftware im eigenen Netz** bereitgestellt, wurde in der Regel unternehmens- oder behördenintern eine Erforderlichkeits- und Risikobetrachtung durchgeführt und ein entsprechendes Konzept erstellt, wie beispielsweise mit Meta-, Protokoll- und Analysedaten umgegangen wird oder welche Funktionen für die Teilnehmenden verfügbar sind. Diese Lösung erlaubt dem Unternehmen oder der Behörde mehr Kontrolle über die Datenverarbeitung als bei einem Online-Dienst und ist daher meistens zu bevorzugen.
  - Wenn Sie keine Software im eigenen Netz nutzen können und die Videokonferenz über einen **Online-Dienst** realisieren, fragen Sie vorab in Ihrem Unternehmen bzw. in Ihrer Behörde nach, ob und welche Videokonferenz-Lösungen infrage kommen. Die Leitung Ihres Unternehmens oder Ihrer Behörde sollte bei dieser Entscheidung gemeinsam mit der IT-Administration und der oder dem Datenschutzbeauftragten allgemeine Fragestellungen – wie beispielsweise Datenverarbeitung im Geltungsbereich der DSGVO, Verwendung datenschutzfreundlicher Voreinstellungen, Einsatz von Verschlüsselung usw. – berücksichtigen und kann sich zusätzlich an den Maßnahmen in dieser Handreichung orientieren.
- **Außerhalb des professionellen Einsatzbereichs** werden Sie in der Regel einen Online-Dienst in Anspruch nehmen. Bevor Sie sich für eine Lösung entscheiden, setzen Sie sich mit den Datenschutz-Anforderungen für Ihren Einsatzzweck auseinander – z. B. anhand der Fragestellungen in dieser Handreichung. Vergleichen Sie auf dieser Grundlage mehr als einen Anbieter. Sie sollten sich ebenfalls mit den teilnehmenden Personen absprechen, ob eine Videokonferenz für den Zweck der Datenverarbeitung angemessen ist. Auch bei der ehrenamtlichen Arbeit z. B. in einem Verein können sensible Daten von anderen Personen betroffen sein.

Voraussetzungen für Videokonferenzen klären



Wenn Ihr Unternehmen oder Ihre Behörde schon einen Videokonferenz-Dienst einsetzt, dann werden die Verwendung und die Verhaltensregeln üblicherweise in einer Richtlinie oder Dienstvereinbarung geklärt sein. Wenn Sie aus spontanen Anlass Videokonferenzen verwenden müssen, können Sie die Empfehlungen dieser Handreichung verwenden.

Bereits bei der **Organisation** einer Videokonferenz sind einige Fragestellungen zu beachten, die für einen datenschutzkonformen Einsatz wichtig sind und die weitere Zusammenarbeit erleichtern können:

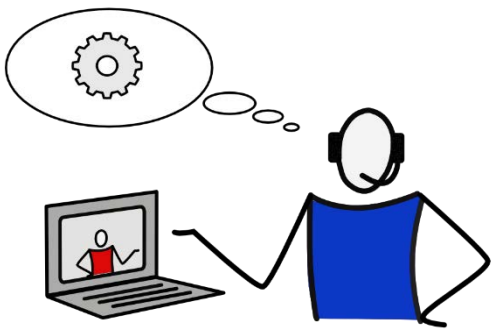
- Wenn bei dem Einsatz vorgesehen ist, dass parallel zur Videokonferenz auch andere Möglichkeiten der Kommunikation (z. B. Messenger) oder der digitalen Zusammenarbeit (z. B. Cloud-Anwendungen) genutzt werden, muss auch dies datenschutzkonform erfolgen.
- Mit der **Auswahl der Software bzw. Technik** für Videokonferenzen sowie bei der Festlegung der Einstellungen können Sie viele datenschutzrechtliche Probleme vermeiden. Die Details finden Sie im nächsten Abschnitt.
  Für die Auswahl der Software bzw. Technik ist oft auch entscheidend, ob die Kommunikation zwischen zwei Personen stattfindet (z. B. in einem Beratungsgespräch) oder in einer Gruppe.

- **Bereiten Sie Ihre Videokonferenz vor**, indem Sie auch den Datenschutz mitdenken, wenn Sie sich nicht sicher sein können, dass ein unbefugter Zugriff über den Dienst oder bei den Teilnehmenden ausgeschlossen ist:
  - Ist für die Teilnahme eine Registrierung bei einem Anbieter erforderlich, kann damit die Weitergabe von personenbezogenen Daten verbunden sein.
  - Soll im Rahmen der Konferenz mit Unterlagen (Dokumente, Präsentationen) gearbeitet werden, können Sie diese z. B. vorab auf sicheren Wegen an die Teilnehmenden verteilen.
  - Soll beispielsweise eine Präsentation im Bild der Videokonferenz gezeigt werden, können Sie personenbezogene Daten in der Präsentation vorher entfernen.
  - Mithilfe von vorab verteilten Unterlagen können Sie bei Bedarf auch Pseudonyme nutzen, die Sie in den Unterlagen festgelegt haben.
- Legen Sie vorab **Regeln für die Teilnahme** fest und informieren Sie die Teilnehmenden rechtzeitig. Dazu gehören insbesondere Moderationsfunktionen (Aufzeichnen, Aufmerksamkeitsanzeige, Stummschalten usw.) und Verhaltensregeln für die Teilnehmenden (z. B. Zulässigkeit von Screenshots oder Aufnahmen). Benennen Sie für Fragen am besten eine Ansprechperson.

Alle **Teilnehmenden** einer Videokonferenz können mit einer guten Vorbereitung zum Gelingen der Konferenz und auch zum Einhalten der Datenschutzvorgaben beitragen:

- Wählen und gestalten Sie bewusst das **Umfeld** für Ihre Teilnahme an der Videokonferenz:
  - Achten Sie darauf, dass im Hintergrund erstens keine persönlichen oder vertraulichen Gegenstände zu sehen sind (z. B. Familienfotos, Arzneimittel, Ordnerrücken mit Klientendaten) und dass zweitens auch nicht zufällig andere Mitglieder des Haushalts bzw. Gäste aufgenommen werden.
  - Wählen Sie besonders im Homeoffice einen Bereich, in dem Sie ungestört sind und die Videokonferenz nicht von anderen im Haushalt bzw. aus der Nachbarschaft mitverfolgt werden kann.
  - Achten Sie darauf, dass Geräte mit Sprachsteuerung (z. B. Smartphones, digitale Assistenten) nicht den Ton der Videokonferenz aufnehmen können.
- Suchen Sie sich eine **geeignete technische Ausstattung** aus und machen Sie sich mit dieser vertraut. So können Kopfhörer bzw. ein Headset verhindern, dass Personen in der Umgebung von Inhalten der Konferenz erfahren.
- Machen Sie sich mit den **Moderationsfunktionen** (z. B. Aufzeichnen der Konferenz oder eine Aufmerksamkeitsüberwachung) und den **Verhaltensregeln** für Teilnehmende vertraut. Beispielsweise sollte geregelt sein, ob Screenshots der Konferenz angefertigt und ggf. sogar in sozialen Medien veröffentlicht werden dürfen – teilen Sie den Wunsch nach einer solchen Regelung ggf. der Ansprechperson mit.

Funktionen von Videokonferenzen einsetzen



Videokonferenzen bringen einige Fragestellungen mit sich …

… für organisierende Personen:

- Videokonferenz-Dienste bringen unterschiedliche Funktionen mit sich. Durch das gezielte Verwenden bzw. Nicht-Verwenden einer solchen Funktion können Sie den Schutz personenbezogener Daten erhöhen. Wird in Ihrem Unternehmen oder Ihrer

Behörde eine On-Premises-Lösung eingesetzt, wurden ggf. einige Funktionen bereits auf Grundlage von Richtlinien konfiguriert. Sie sollten als organisierende Person sowohl im beruflichen Einsatzbereich als auch außerhalb die Verwendung der angebotenen Funktionen daraufhin überprüfen, ob eine datenschutzfreundliche Voreinstellung möglich ist, z. B.:

- **Aufnahme/Speicherung** einer Videokonferenz („Protokoll", „Archivierung")
  Videokonferenz-Lösungen können Aufnahmefunktionen anbieten, die den Verlauf der Videokonferenz in Ton und Bild aufzeichnen. Auch wenn Ihnen diese Funktion verlockend erscheint: Es gibt in der Regel immer datenschutzfreundlichere Lösungen als eine umfangreiche Aufzeichnung von Wort und Bild inklusive Gestik und Mimik, z. B. schriftliche Protokolle, wie sie auch in nicht-elektronischen Meetings zum Einsatz kommen. Bei einer Speicherung/Archivierung müssen u. a. Zugriffsberechtigungen, Löschfristen und die Wahrung der Betroffenenrechte gewährleistet werden. Die Risiken im Zusammenhang mit der Speicherung und die möglichen technischen und organisatorischen Maßnahmen müssen im Vorfeld betrachtet und festgelegt werden.
- **Integration von sozialen Medien**
  Videokonferenz-Lösungen können die Integration von sozialen Medien (Social Media) anbieten. Achten Sie bei der Einbindung solcher Inhalte darauf, dass Sie dabei keine sensiblen Daten anderer Personen offenlegen. Achtung: Einige Videokonferenz-Dienste nehmen automatisch Kontakt zu Social-Media-Plattformen auf – das ist jedoch in der Regel weder nötig noch gewollt.
- **Aufmerksamkeitsanzeige**
  Einige Videokonferenz-Lösungen bieten Aufmerksamkeitsanzeigen, die es ermöglichen sollen, zu erkennen, ob Teilnehmende der Videokonferenz folgen. Diese Überwachung ist ein Eingriff in die Persönlichkeitsrechte der Teilnehmenden! Aktivieren Sie die Funktion nur, wenn es zwingend notwendig ist, z. B. bei Online-Seminaren mit Teilnahmenachweis. Auf jeden Fall müssen Sie darüber vorab informieren.
- **Passwortschutz/Anklopfen**
  Wenn die Videokonferenz-Lösung die Möglichkeit bietet, einen Konferenzraum zu sperren und eine Teilnahme erst nach einer Eingabe eines Passworts bzw. nach einem „Anklopfen" (auch: Warteraum) und Freigabe der Teilnahme durch die Moderation zu erlauben, dann verwenden Sie diese Funktion. Damit können Sie erreichen, dass nur berechtigte Personen an Ihrer Videokonferenz teilnehmen.

- Um die **Transparenz** der Datenverarbeitung in Ihrer Videokonferenz zu gewährleisten bzw. die Teilnehmenden über die Verwendung ihrer Daten zu informieren, sollten Sie
  - den Teilnehmenden Ihrer Videokonferenz die Möglichkeit geben, Ihre Datenschutzerklärung oder Datenschutz-Kurzinformation („Datenschutz-Steckbrief" – Link zur Vorlage siehe „Quellen und weitere Informationen") einzusehen oder herunterzuladen, z. B. von Ihrer Webseite, oder
  - den Teilnehmenden Ihrer Videokonferenz die datenschutzfreundliche Verwendung der Funktionen vor Beginn der Videokonferenz zu erläutern oder die Chatfunktion zu benutzen, um die datenschutzrelevanten Informationen dort bereitzustellen. Dazu können Sie eine Textvorlage erstellen, die sich für jede Videokonferenz eines entsprechenden Anbieters verwenden lässt.
  - Sollten Sie Funktionen verwenden, mit denen ein erhöhtes Risiko verbunden ist (Aufnahme, Aufmerksamkeitsanzeige, kein Passwortschutz usw.), informieren Sie darüber deutlich im Vorfeld.

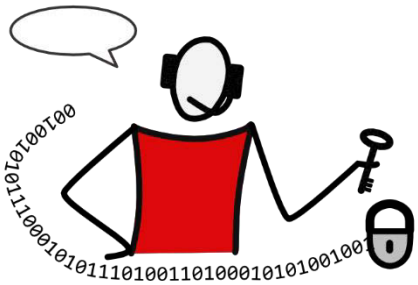
- Überlegen Sie, ob Sie die Identität der Teilnehmenden der Videokonferenz prüfen müssen, um zu gewährleisten, dass keine Unbefugten teilnehmen. Bei der Verwendung eines komplexen Passworts beim Zugang kann dies schon sichergestellt sein.
- Bereiten Sie sich auf **mögliche Datenschutz-Probleme** vor, die im Laufe der Videokonferenz auftreten können:
  - Überlegen Sie sich Ihre Reaktion als Moderation, wenn einzelne Teilnehmende unerlaubt personenbezogene Daten verwenden oder veröffentlichen.
  - Bereiten Sie einen Plan B vor, falls technische Probleme auftauchen – beispielsweise eine Terminverschiebung oder das Ausweichen auf eine Telefonkonferenz.
  - Falls die Videokonferenz nicht durch ein Passwort o. ä. geschützt ist, sollten Sie schnell reagieren, falls eine unberechtigte Person an der Konferenz teilnimmt.

… für **teilnehmende Personen**:

- **Überprüfen** Sie bei Beginn der Videokonferenz, welche Funktionen die Videokonferenz-Software zur Verfügung stellt und ob Funktionen deaktiviert wurden, z. B. ausgegraut oder entsprechend markiert, oder ob bestimmte Voreinstellungen bei den Funktionen vorgenommen wurde, z. B. ausgeschaltete Kamera oder ausgeschaltetes Mikrofon.
- **Informieren** Sie sich im beruflichen Einsatzbereich bei der organisierenden Person, ob für die Datenverarbeitung im Zusammenhang mit der Videokonferenz eine Datenschutzerklärung oder eine Datenschutz-Kurzinformation bereitgestellt wird. Sollten diese Informationen nicht vorhanden sein, dann bitten Sie bei Unklarheiten die organisierende Person, die Regelungen zur Verwendung der verschiedenen Funktionen zu erläutern.
- **Testen** Sie die Funktionen, mit denen Sie Ihre Privatsphäre schützen können, um sie während der Videokonferenz sicher verwenden zu können, z. B. Deaktivierung von Ton und/oder Bild.
- Sollten Sie Teile der Videokonferenz für die eigene Nachbereitung aufzeichnen oder z. B. Screenshots für die Veröffentlichung in sozialen Medien erstellen wollen, stellen Sie unbedingt sicher, dass dies ausdrücklich erlaubt ist und die anderen Teilnehmer eingewilligt haben.

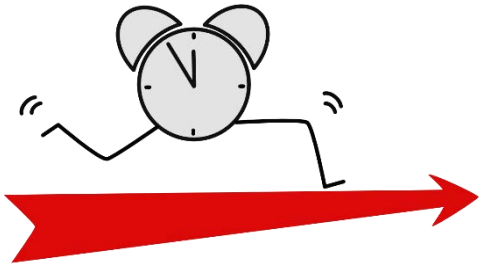
In Videokonferenzen datenschutzfreundlich verhalten

Wenn Sie an einer Videokonferenz teilnehmen, können Sie durch Ihr eigenes Verhalten vermeiden, dass sensible Informationen weitergegeben werden:



- Seien Sie sich bewusst, dass in einer Videokonferenz alle anderen Teilnehmenden zuhören, und geben Sie keine sensiblen Informationen weiter.
- Nutzen Sie beispielsweise externe oder auch integrierte Direkt-Chats, um mit einzelnen Personen Informationen austauschen zu können, die nicht an alle Teilnehmende gerichtet sind.
- Schalten Sie Ihr Mikrofon stumm und ggf. die Kamera aus, z. B. wenn im Homeoffice andere Personen aus Ihrem Haushalt in den Aufnahmebereich des Mikrofons oder in das Sichtfeld der Kamera kommen. Ein Schild an der Tür im Homeoffice kann über laufende Konferenzen informieren, damit ein „Hineinplatzen“ vermieden wird.

- Seien Sie in der Videokonferenz aufmerksam und informieren Sie die organisierende Person bzw. die anderen Teilnehmenden, wenn beispielsweise eine fremde Person den Konferenzraum betritt oder ohne Vorankündigung und Absprache eine Aufnahme der Videokonferenz gestartet wird.



Wenn es länger als „kurzzeitig“ dauert

Wenn Sie Videokonferenzen spontan einsetzen mussten, um mit Ihren Kollegen, Klienten, Mitgliedern usw. im Kontakt zu bleiben, und noch keine konzeptionelle Grundlage für diese Verarbeitungstätigkeit haben, können Sie kurzzeitig die hier beschriebenen Hinweise verwenden, um wichtige Anforderungen an die Datenschutzkonformität bei Videokonferenzen umzusetzen.

Generell ist es aber notwendig, eine der Datenverarbeitung angemessene Erforderlichkeits- und Risikobetrachtung durchzuführen, auf deren Basis eine geeignete Videokonferenz-Lösung auszuwählen sowie technische und organisatorische Maßnahmen zu Datenschutz und Datensicherheit festzulegen und zu dokumentieren.

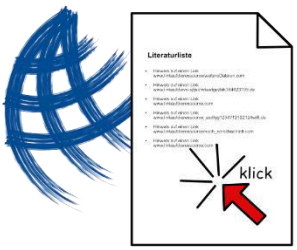
Anhang: Beispiele für Einsatz-Szenarien

Videokonferenzen kommen in verschiedenen Szenarien zum Einsatz, die wiederum unterschiedliche Anforderungen an den Datenschutz stellen:

- **Berufliche Videokonferenzen** innerhalb eines Unternehmens oder einer Behörde oder ggf. mit Mitarbeitenden aus anderen Unternehmen oder Behörden dienen als Ersatz für Besprechungen. Um den Beschäftigtendatenschutz zu gewährleisten, ist in der Regel eine Betriebs- oder Dienstvereinbarung erforderlich.
- **Video-Beratungen**, die von einem Unternehmen oder einer Behörde für Privatpersonen angeboten werden, stellen nicht nur die genannten Anforderungen an den Beschäftigtendatenschutz, sondern es muss auch der Datenschutz der Beratenen berücksichtigt werden. Wichtig ist eine umfassende und verständliche Information der Beratenen über die Verarbeitung ihrer Daten und über ihre Rechte. Der Einsatz im Gesundheitswesen (z. B. im Rahmen von Telemedizin) und in anderen besonders sensiblen Bereichen unterliegt speziellen Anforderungen.
- **Videokonferenzen in Bildungseinrichtungen** unterliegen speziellen Anforderungen, besonders im schulischen Bereich. Detaillierte Informationen und eine ständig aktualisierte Positivliste gibt es auf https://medienberatung.iqsh.de/corona2.html
- **Videokonferenzen im Ehrenamt** (z. B. in Vereinen oder kommunalen Ehrenämtern) bedürfen der informierten Einwilligung der Beteiligten. Gegebenenfalls sind vorab auch Satzungsänderungen oder andere Beschlüsse notwendig, bei denen Interessenvertretungen einzubinden sind.
- **Rein private Videokonferenzen** bspw. zwischen Familienangehörigen liegen zwar nicht im Anwendungsbereich der Datenschutz-Grundverordnung, doch können einige dieser Hinweise trotzdem von Interesse sein.

In der Praxis treten die Szenarien teilweise kombiniert auf und weisen im Einzelfall noch komplexere Anforderungen auf.

Quellen und weiterführende Informationen



- **Nutzung von Messenger- und Videokonferenzdiensten in Zeiten der Corona-Pandemie**
  Information des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
  Stand: April 2020, deutsch
  https://www.bfdi.bund.de/DE/Datenschutz/Datenschutz-Corona/Kommunikation/Inhalt/Messenger_Videokonferenzdienste.html
- **Leitfragen zur Beurteilung von Angeboten**
  Information des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
  Stand: April 2020, deutsch
  https://www.bfdi.bund.de/DE/Datenschutz/Datenschutz-Corona/Kommunikation/Inhalt/Beurteilung_Angebote_Messenger.html
- **Kompendium Videokonferenzsysteme**
  Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
  Stand: April 2020, 173 Seiten, deutsch
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf
- **Datenschutzfreundliche technische Möglichkeiten der Kommunikation**
  Artikel des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg
  Stand: März 2020, deutsch
  https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/
- **Praxishilfe „Videokonferenzen und Datenschutz“**
  Praxishilfe der Gesellschaft für Datenschutz und Datensicherheit e.V.
  Stand: April 2020, 17 Seiten, deutsch
  https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_xvi-videokonferenzen-und-datenschutz
- **Einsatz von digitalen Angeboten während der Corona-Krise**
  Information des Instituts für Qualitätsentwicklung an Schulen Schleswig-Holstein (IQSH)
  laufend aktualisiert, deutsch
  https://medienberatung.iqsh.de/corona2.html
- **COVID-19 : les conseils de la CNIL pour utiliser les outils de visioconférence**
  Information der Commission Nationale de l’Informatique et des Libertés (CNIL) aus Frankreich
  Stand: April 2020, französisch
  https://www.cnil.fr/fr/covid-19-les-conseils-de-la-cnil-pour-utiliser-les-outils-de-visioconference
- **Informationspflichten mit dem „Datenschutz-Steckbrief“**
  Umsetzung der Informationspflichten nach Art. 13 und Art. 14 DSGVO
  Stand: April 2020
  https://www.datenschutzzentrum.de/dokumentation/

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Telefon: 0431 988-1200
E-Mail: mail@datenschutzzentrum.de