

Virtuelle Kommunikation
funktioniert ;)

Digitale Zusammenarbeit im Spannungsfeld von Kommunikationschancen und Datenschutzrisiken

Eine Hilfestellung zur differenzierten Betrachtung von Vorgehensweisen bei Videokonferenzen

Frank Ulmer • Robert Müller-Török • Anna Deckert • Carsten Ulbricht

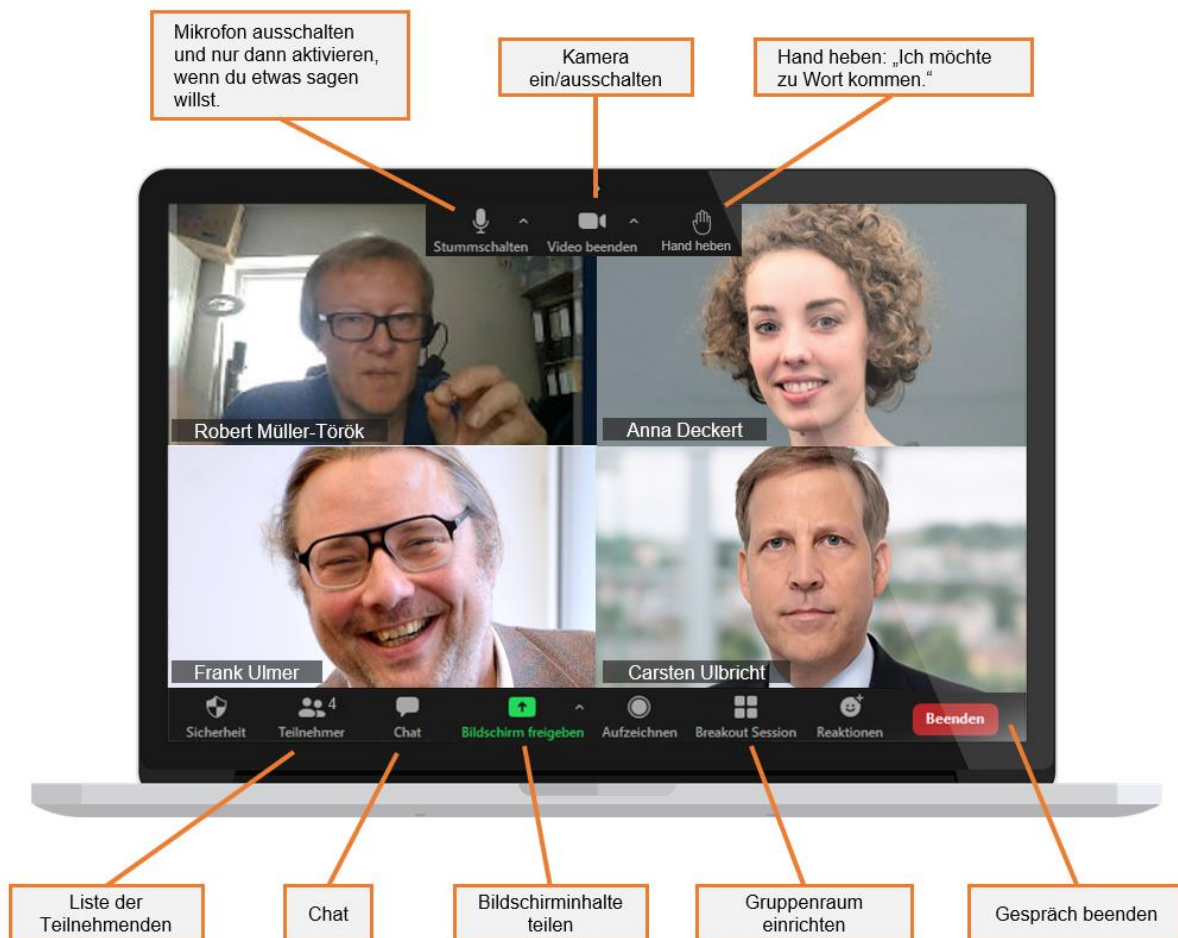


Abb. 1: Übersicht Videokonferenztools mit Bildern der Autor/innen

Im Zeitalter der Digitalisierung ist der Bedarf an Stakeholder-Beteiligung hoch. Egal ob es um den Mobilfunkstandard 5G oder um Datenschutz geht. Aus dem Zitat »Man kann nicht nicht kommunizieren!« ergibt sich die Notwendigkeit für Onlinedialoge – denn auch entfallene Dialoge sind eine Form der Kommunikation.

Aber wie umsetzen, während man sich COVID-19-bedingt nicht treffen kann oder zukünftig weniger treffen will, um ökologische und finanzielle Kosten einzusparen?

In der Beratung der öffentlichen Verwaltung hört man immer öfter den Satz »erst die Strukturen, dann die Tools«. Das gilt auch für die Bewertung von Videokonferenzoptionen: Erst den Anwendungsfall, die Ziele und den Bedarf spezifizieren – dann über die Technik und Tools nachdenken. Ansonsten gilt leider auch in diesem Bereich das englische Sprichwort »A fool with a tool is still a fool«.

Mit Beginn der COVID-19-Krise sind viele Unternehmen verstärkt in die virtuellen Welten eingestiegen (1). Kommunen, Ministerien und Behörden haben die Videotools für interne Abstimmungen entdecken müssen, aber Dialogveranstaltungen mit Stakeholdern oder der breiten Öffentlichkeit häufig abgesagt oder vertagt. Auch weil die erste, zumeist hemdsärmelige und unter Zeitdruck erfolgte Risikoabschätzung zu Online-Dialog-Tools negativ ausging oder nicht belastbar genug erschien, fand ein öffentlicher Diskurs über diese Tools nicht statt.

Mit diesem Beitrag möchten wir Orientierung in zwei Bereichen stiften: 1) Wie ist die Rechtslage für den Einsatz von Video-Konferenztools? Und: 2) Welche praktischen Fragen sind bei der Planung und Umsetzung von Online-Dialogen zu beachten? Lassen Sie uns mit der zweiten Frage beginnen.

Praxis-Tipps für den Einsatz von Videokonferenztools für Online-Dialoge



Die Regel »jeder Dialog ist ein Unikat« gilt auch für größere »Online-Dialoge«. Beteiligungsforschende wissen schon lange, dass jeder Dialog einzigartig ist und jedes Mal grundsätzlich jeweils neu zu entscheiden ist, welches Medium und welche Vorgehensweisen am besten passen. Deshalb ist es sinnvoll, sich bei der Suche nach einem geeigneten Videokonferenztool ebenso auf den Einzelfall zu beziehen.

Davor sollte man sich vor Augen führen, wie solche Tools funktionieren. Sie haben im Unterschied zu großen Veranstaltungen in der realen Welt einige Eigenschaften, die sie nicht als 1:1-Substitut für das COVID-19-induziert verbotene »Townhallmeeting« qualifizieren. Einige dieser Eigenschaften sind:

- Da bei vielen Systemen mehr als zehn oder zwölf Kamerabilder nicht eingeblendet werden können – die Bildschirmgröße oder technische Möglichkeit beschränkt dies – sind die allermeisten Teilnehmenden häufig »gesichtslos« – so ist weder ein vergleichbares Gemeinschaftsgefühl noch ein Rückschluss von ihrer Mimik möglich
- Ebenso sind die Teilnehmenden regelmäßig standardmäßig allesamt stumm geschaltet, damit Hintergrundgeräusche wie klingelnde Telefone das Veranstaltungsgeschehen nicht stören.
- Die Moderierenden haben im Tool eine Macht, die im realen Meeting nicht existiert. Unangenehme Zwischenrufer mit einem Mausklick völlig stumm, taub und blind zu schalten oder aus dem Meeting zu werfen ist in der realen Welt unmöglich.

- Die Teilnahme ist ortsungebunden. Das kann dazu führen, dass sich nicht nur lokal ansässige Stakeholder einwählen, sondern illegitimer Weise ggf. auch deren überregionale Unterstützer oder Gegner. Ganz nach dem Motto »Bring your own claue«.
- Verewigt im Internet. Falls das Video live gestreamt wird, also jedem in Echtzeit oder im Nachgang dauerhaft zugänglich gemacht wird, sind die Inhalte für immer für die Nachwelt verfügbar. Zum Schutz der oft ungeübten Teilnehmenden kann deshalb die Einwahl eines begrenzten Personenkreises deutlich attraktiver sein - ohne die öffentliche Bereitstellung Internet. Oder das Abschalten des Videobildes angeboten werden.

Soll nun also eine Videokonferenz einen »vor Ort«-Diskurs ersetzen und online ein vergleichbarer Schutz der Persönlichkeitsdaten der Gäste gewährleistet werden, so bietet die folgende Checkliste Prüfkriterien, anhand derer abgeleitet werden kann, ob das zur Diskussion stehende Videotool und die entsprechende Vorgehensweise die Anforderungen erfüllt.

Wünschenswerter Aspekt	 Vor Ort	 Online
1. Inklusivität & Barrierefreiheit	<ul style="list-style-type: none"> ▪ Ebenerdige Räume, breite Toiletentüren, ▪ Übersetzung / Gebärdendolmetscher/in etc. 	<ul style="list-style-type: none"> ▪ Telefoneinwahl ermöglichen ▪ Beitritt ohne eigene Mailadresse ermöglichen ▪ Beitritt ohne Installation einer Software ermöglichen
2. Flexibilität	<ul style="list-style-type: none"> ▪ Lassen Sie sich auf Extrawünsche ein? Wenn jemand Lactose-Intoleranz oder Gluten-Allergie hat? 	<ul style="list-style-type: none"> ▪ Für Menschen, die am Online-Leben legitimerweise nicht partizipieren wollen: Wählen Sie ein Format, bei dem man sich telefonisch einbinden kann. Alternativ können Sie zusätzlich im Vorfeld Fragen/Themen bei den Teilnehmenden einholen.
3. Stressreduktion	<ul style="list-style-type: none"> ▪ Es werden angemessene Pausen geplant. ▪ Wir achten auf Akustik. ▪ Kleingruppenarbeit in unterschiedlichen Räumen 	<ul style="list-style-type: none"> ▪ Die Tagungszeit etwas kürzer wählen ▪ Pausen machen ▪ Netiquette erläutern (Mikrofone aus etc.)
4. Geeigneter Teilnehmendenkreis	<ul style="list-style-type: none"> ▪ Wer darf kommen? Wer bekommt Veranstaltungsort und -zeit mitgeteilt? 	<ul style="list-style-type: none"> ▪ Überlegen Sie, wem Sie den Zugangslink geben und ob die Konferenz passwortgeschützt ist oder nicht.

<p>5. Atmosphäre</p>	<ul style="list-style-type: none"> ▪ Sie bemühen sich, dass es schön aussieht (Dekoration, Verpflegung, etc.) ... ▪ und alle sich wohl fühlen (erkennbare Ansprechpersonen, geübte Moderation, gut ersichtliche Tagesabläufe) 	<ul style="list-style-type: none"> ▪ Im Vorfeld Anregungen rund senden, wie die persönliche Video-Präsentation gut aussieht (Vermeiden von Fehlern wie Über- und Unterbelichtung; unpassender Hintergrund) ▪ Check-in: Persönlichen Austausch über Chat anregen / auffordern, sich ein Getränk zu holen, interaktive Abfrage von Herkunftsorten, Institutionen, etc. ▪ Erkennbare technische Ansprechpersonen und geübte Moderation sicherstellen
<p>6. Angemessene Methodik</p>	<ul style="list-style-type: none"> ▪ Viele Räume oder wenige Räume? Muss jeder zu Wort kommen? Frontal? Kleingruppen? ▪ Will ich spontan weitere Räume anbieten können wie bei einem Open Space? 	<ul style="list-style-type: none"> ▪ Sich selbst fragen: Brauche ich Kleingruppen? Brauche ich für diese auch digitale Metaplanwände, die ich nachher zusammenführen kann? Muss das Tool auch spontane Kleingruppenarbeit (sog. <i>Break Out Sessions</i>) ermöglichen? ▪ Verwenden Sie Online-Metaplanwand-Tools. So können die Teilnehmenden Gedanken notieren und teilen.
<p>7. Schutz von Persönlichkeitsrechten</p>	<ul style="list-style-type: none"> ▪ Sollen Fotos veröffentlicht werden? → Schriftliche Zustimmung einholen ▪ Bei der Registrierung bleibt die Eintragung in eine Teilnehmerliste freiwillig 	<ul style="list-style-type: none"> ▪ Wenn Screenshots mit Aufnahmen von Gesichtern veröffentlicht werden sollen oder die ganze Konferenz live gestreamt wird → Zustimmung vorab einholen (Sichtbarkeit von Namen auf Bildern vermeiden) ▪ Registrierung ohne Emailadresse bzw. anonym über Telefonwahl möglich machen ▪ Klarnamen oder Alias als sichtbarer Benutzernamen zur Auswahl stellen
<p>8. Regionale Versorgung</p>	<ul style="list-style-type: none"> ▪ Verpflegung mit regionalen Speisen & Getränken 	<ul style="list-style-type: none"> ▪ regionale Anbieter von Videokonferenzsystemen in Betracht ziehen (teilweise sind diese teurer oder weniger komfortabel)

Abb. 2: Checkliste mit Prüfkriterien für Videotools

Insbesondere auf den Aspekt »Schutz der Persönlichkeitsrechte« möchten wir im Weiteren näher eingehen.

Rechtliche Anforderungen an den Einsatz von Videokonferenztools

Der Schutz persönlicher Daten ist eines der wichtigsten und zentralsten Themen unserer Zeit und darf keinesfalls auf die leichte Schulter genommen werden. Gerade deshalb ist eine übersichtliche und zugleich differenzierte Darstellung wichtig. Das Gegenteil aber ist geschehen: Viele auf unvollständigem Wissen beruhende Vorverurteilungen und wenig differenzierte Blicke auf Datenschutz und Datensicherheit waren in den Medien sichtbar. Videokonferenzsysteme wurden sehr pauschal als ungeeignet bewertet, obwohl die Risikoforschung das Gegenteil – Einzelfallbewertungen und Risikovergleiche statt einer isolierten Betrachtung – empfiehlt. Eine vergleichende Risikobewertung ist facettenreicher und liefert oftmals ein klareres Bild. Dabei stehen Fragen wie diese im Fokus: »Wie viel weniger oder mehr verletzlich sind meine Daten im E-Mail-Postfach (oder auf WhatsApp, Facebook etc.) im Vergleich zu einer Videokonferenz?« oder »Wie groß ist unser Schaden, wenn auf Kosten der Einhaltung von Datenschutzregeln der Diskurs in unserer pluralisierten Welt wegfällt?«. Diese abwägenden Fragen machen deutlich, über welche Gefahren und Risiken wir eigentlich sprechen sollten. Sie stellen keine Grundlage für eine datenschutzrechtliche Beurteilung dar.

Wie wählt man nun ein geeignetes Tool aus? Eine strukturelle Herausforderung bei der Entscheidung für oder gegen den Einsatz bestimmter Online-Tools ist, dass die Beauftragten für Datenschutz durch die EU-Datenschutzgrundverordnung (DSGVO) in den Institutionen und Verwaltungen bereits seit deren Verabschiedung regelmäßig fachlich überfordert wurden (zur DSGVO siehe Absatz rechtliche Anforderungen). Es ist ihnen – oftmals auf Grund fehlender fachlicher Kenntnisse – gar nicht möglich, selbst prüfend tätig zu werden, und so müssen oft schnell »ergoogelte« Fremdeinschätzungen das fundierte eigene Urteil ersetzen. Eine weitere strukturelle Herausforderung ist, dass beim staatlichen Handeln stets die Maxime gilt, rechtskonform zu handeln; privatrechtliche Organisationen können hingegen oftmals abwägen und mögliche Sanktionen in Kauf nehmen. Das geforderte rechtskonforme Handeln ist in einer Welt schwierig geworden, die teilweise sehr verzögert dann aber auch mit hastig verabschiedeten Gesetzen oder auch nur Verordnungen auf neue Realitäten wie die COVID-19-Krise – oder auf technologischen Entwicklungen – reagiert.

Um die spannenden Optionen, die der Einsatz von Videokonferenztools für Institutionen, aber gerade auch für die öffentlichen Verwaltung bietet, sinnhaft und rechtskonform zu nutzen, müssen nichtsdestotrotz einige grundsätzliche Anforderungen der seit zwei Jahren geltenden Datenschutzgrundverordnung (DSGVO) beachtet werden.

Die Erfahrung zeigt, dass verschiedene Videokonferenzlösungen – trotz immer wieder geäußerter Bedenken – auch seitens öffentlicher Stellen durchaus datenschutzkonform eingesetzt werden können (2).

Bei Beachtung der nachfolgenden Voraussetzungen ist der Einsatz von Videokonferenzen für den Online-Dialog aus rechtlicher Sicht grundsätzlich zulässig.

1. Legitimation der Datenverarbeitung und Nutzungskonzept

Im Rahmen der Kommunikation über Videokonferenztools werden stets auch personenbezogene Daten der Teilnehmer/innen verarbeitet. Dies ist datenschutzrechtlich aber nur zulässig, wenn einer der sogenannten Legitimationstatbestände des Art. 6 DSGVO die Verarbeitung erlaubt.

Bei öffentlichen Stellen kann hier Art. 6 Abs.1 lit.e DSGVO in Verbindung mit § 3 BDSG bzw. der entsprechenden Regelung aus dem Landesdatenschutzgesetz (in Baden-Württemberg etwa § 4 LDSG)

herangezogen werden. In entsprechenden Fällen lässt sich nämlich gut begründen, dass der Einsatz von Videokonferenzen für den Online-Dialog und für eine (moderne) Verwaltungskommunikation heutzutage auch erforderlich ist. Zweck, Art und Umfang der vorgesehenen Nutzung sollten dementsprechend in einem Konzept niedergelegt werden.

Alternativ wäre wohl auch denkbar, dass die Teilnehmer/innen in die Datenverarbeitung des jeweiligen Videokonferenztools einwilligen.

2. Auswahl des Dienstes

Nach Erstellung des Nutzungskonzeptes sollte ein geeigneter Videokonferenzdienst ausgewählt werden.

Dabei könnte zunächst in Erwägung gezogen werden, ob eine On-Premise-Variante (also auf den eigenen Servern gehostete Software) in Frage kommt. Dies stellt grundsätzlich die datenschutzfreundlichste Variante dar, da bei einer solchen Lösung die Kontrollmöglichkeiten über die Datenverarbeitungsvorgänge am besten gewährleistet werden kann. Beim Einsatz von Videokonferenztools von Drittanbietern als SaaS (Software as a Service) im Rahmen von Cloud-Lösungen sind EU-Dienste vorzuziehen.

Wenn das zu aufwändig erscheint, ist unter den nachfolgenden Voraussetzungen aber auch der Einsatz bestehender US-basierter Videokonferenzanbieter wie Zoom, MS Teams & Co denkbar.

3. Abschluss eines Auftragsverarbeitungsvertrages

Beim Einsatz solcher Videokonferenzanbieter ist davon auszugehen, dass diese die personenbezogenen Daten (z.B. der Teilnehmer) im Auftrag der jeweiligen öffentlichen Stellen verarbeitet.

Damit sind diese Anbieter grundsätzlich als Auftragsverarbeiter anzusehen. Demgemäß sollte mit diesen ein Vertrag über die Auftragsverarbeitung nach Maßgabe des Art. 28 DSGVO geschlossen werden.

Da einige der gängigen Anbieter den Abschluss eines solchen Auftragsverarbeitungsvertrages im Rahmen der eigenen Standardverträge auch bereits anbieten, lässt sich diese Anforderung ebenfalls erfüllen.

4. Datenschutzniveau bei Diensten aus Drittstaaten

Wenn Dienste aus Ländern außerhalb der EU (sog. Drittstaaten) eingesetzt werden sollen, muss zusätzlich sichergestellt werden, dass das dortige Datenschutzniveau den Anforderungen der DSGVO entspricht.

Auch hierfür gibt es Umsetzungsoptionen, die von einigen Anbietern erfüllt werden. Bei Unternehmen aus den USA würde es ausreichen, wenn diese nach dem EU-US-Privacy-Shield zertifiziert sind. Ob dies der Fall ist, kann für den konkreten US-Dienstleister unter <https://www.privacyshield.gov/list> geprüft werden. Ansonsten können mit dem Anbieter auch die sog. Standarddatenschutzklauseln nach Art. 46 DSGVO abgeschlossen werden, die den Vertragspartner zur Einhaltung des europäischen Datenschutzniveaus vertraglich binden.

5. Datensicherheit

Vor Einsatz eines Videokonferenztools sollte außerdem sichergestellt werden, dass der Anbieter ausreichende technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten trifft (z.B. Pseudonymisierung, Backup, Verschlüsselung etc.). Auf den Webseiten der Anbieter finden sich häufig Informationen zum Stand der Datensicherheit.

Zusätzlich sollten selbst folgende organisatorische Maßnahmen getroffen werden:

- Zutritt der Teilnehmer nur mit Passwort
- Zugangslinks nie öffentlich bekanntgeben
- Zutritt der Teilnehmer erst nach Beitritt des Veranstalters ermöglichen
- Sperrung für nicht geladene Teilnehmer nach Eröffnung

6. Datenschutzhinweise

Schließlich sind die Kommunikationsteilnehmer nach Art. 13 DSGVO im Rahmen eines Datenschutzhinweises über die stattfindenden Verarbeitungsprozesse beim Einsatz des Videokonferenztools zu informieren.

Zusammenfassend lässt sich also feststellen, dass der Einsatz solcher Videokonferenztools auch für die öffentliche Verwaltung durchaus denkbar ist, wenn der Anbieter entsprechend der obenstehenden Vorgaben ausgewählt, und die aufgezeigten datenschutzrechtlichen Anforderungen auch entsprechend umgesetzt werden.

7. Schlussfolgerungen

Die Anwendung von Videokonferenzen ist ein Beispiel für eine sich durch Digitalisierung verändernde Gesellschaft und Demokratie.

Was für Videokonferenzen gilt, steht für die gesamte Digitalisierung: Eine schlecht gemachte Digitalisierung ist der Brandbeschleuniger für die Verstärkung vieler ökologischer, ökonomischer und sozialer Ungerechtigkeiten und Probleme. Andersrum: Digitalisierung klug ausgestaltet birgt große Chancen in vielen Dimensionen: Eine gut gemachte Videokonferenz in der passenden Situation hat große Mehrwerte. Diskurse zu ermöglichen ist eines der Standbeine, um nachhaltige Entwicklung zu ermöglichen – auch digitale Entwicklung – trotz ansteigenden Stromverbräuchen.

Um die Digitalisierung als Chance für eine nachhaltige Entwicklung nutzen zu können, ist es notwendig, dass Kommunen, Behörden und Ministerien reaktionsschneller werden, um auf eine sich verändernde Mitwelt zu reagieren. Digitalisierung sollte dafür auch interministeriell gestaltet werden und kann nicht durch kleinteilige Rechtsprüfungen bewerkstelligt werden. Ein interministerielles, klares Konzept für ein besseres Leben durch Digitalisierung wäre hier wünschenswert.

Gerade im Kontext von Bürgerbeteiligung und Stakeholder-Dialogen wäre der Staat in der Pflicht: Für Besprechungen mit besonderem Sicherheitsbedürfnis (das ist in der Regel nicht der Stakeholder-Dialog) sollte eine unabhängige digitale Infrastruktur genutzt werden. Idealerweise betreibt diese der Staat oder man hostet sie selbst (Betrieb auf eigenen Servern). Zum Vergleich: Es gibt gute Gründe dafür, warum die Informationsübermittlung (Post) sehr lange Zeit staatliche Aufgabe war.

»Bremse der Digitalisierung« auch in diesem Kontext bleibt, dass der Bund die Online-Authentifizierung nicht bereitstellt; also die Möglichkeit, Bundesbürger/innen auch online eindeutig erkennen zu können. Das würde eine weitreichende Beschleunigung auf dem Weg in eine neue digitalisierte Welt bieten. Bei Videokonferenzen würden auf diese Weise eine Festlegung der Teilnehmerstruktur und Abstimmungen ermöglicht. Ganz abgesehen davon, dass dadurch der Online-Behördengang möglich wird. Auch viele Ergebnisse von Online-Bürgerbeteiligungsprozessen wären belastbarer, da es sich um »echte« Einwohner/innen handelte.

Bürgerinnen und Bürger wie auch Unternehmen sind unseres Erachtens bereit für diesen Aufbruch, digital zu denken und zu handeln. Sie haben bereits jetzt viele Mehrwerte für sich und die Umwelt und die Innovationskraft durch manche entfallene Anreise zu Meetings und Veranstaltungen erlebt.

Die Umsetzung Ihres Video-Dialogs kann gelingen, wenn Sie die in der Checkliste genannten Aspekte bedenken: Denken Sie daran, vor jedem Online-Meeting den Teilnehmenden klar zu machen, worauf sie sich »einlassen«. Diese können dann die Vor- und Nachteile eines Online-Dialogs abwägen. Kommunizieren Sie den Teilnehmer/innen explizit die für Ihr Format wichtigsten Aspekte aus der Checkliste. Informieren Sie beispielsweise vorab darüber, dass die Namen der Teilnehmenden während der Konferenz für alle sichtbar sind, dass man das Video an- oder ausmachen kann, ob und wie eine mögliche Aufzeichnung der Konferenz später veröffentlicht wird usw.

Abschließend sind Videokonferenz in der Stakeholder- und Bürgerbeteiligung aus unserer Sicht sehr gut vertretbar – auch vor dem Hintergrund der Risikominimierung und des Datensparsamkeitsgebots.

Wer möchte am Donnerstag, den 20. August 2020 von 14:00 bis 15:30 Uhr in einer Videokonferenz mit den Autoren diskutieren?

Um was es geht bestimmen Sie. Die Videokonferenz wird nicht aufgezeichnet und nicht live gestreamt. Ausschließlich die ausgewählten Personen werden sich gegenseitig sehen. Die Aktivierung der Kamera ist keine Voraussetzung. Sie müssen sich allerdings mit ihrem Klarnamen unter post@kommunikationsbuero.com anmelden, damit alle Diskutanten »sehen« können, wer mit Ihnen im Raum ist. Die Namen werden ausschließlich an alle Mitdiskutanten weitergegeben.

Anmerkungen

(1) Hierzu ein Hinweis: Im Planungssicherstellungsgesetz sind Telefon-/Videokonferenzen jetzt auch für formale Verfahren (v.a. Erörterungstermin) nach § 5(4) und (5) zeitlich befristet bis 31.3.2021 erlaubt.

(2) Vgl. dazu bspw.: <https://www.ecampus-services.uni-bonn.de/de/nachrichten/zoom#7> oder <https://www.cms.hu-berlin.de/de/dl/multimedia/bereiche/tele/zoom/sicherheit> oder <https://rrzk.uni-koeln.de/support-information/informationen-zu-tools-fuer-kollaboratives-arbeiten/zoom-datenschutz-und-nutzungsvorgaben-fuer-hosts-moderatorinnen>

Autor/innen

Frank Ulmer unterstützt mit der Kommunikationsbüro Ulmer GmbH Kommunen, Land und Unternehmen bei der (digitalen) Transformation für mehr nachhaltige Entwicklung. Gleichzeitig forscht er bei der gemeinnützigen Forschungseinrichtung Dialogik gGmbH zu unterschiedlichen Mechanismen die diese Transformation befördern. Seine Fachkompetenz liegt hier auf der Entwicklung und Umsetzung von Stakeholder Dialogen, der Transformation des Energiesystems mittels Wasserstoffs, der Nachhaltige Entwicklung und der Begleitung des Ausbaus des 5G-Netzes mittels partizipativer Methoden.

Robert Müller-Török ist seit 2012 Professor für e-Government an der Hochschule Ludwigsburg und Mitglied des Vorstandes der Österreichischen Computergesellschaft. Seine Forschungsinteressen sind e-Government, e-Democracy und ERP-Systeme, wozu e-Learning und Videokonferenzsysteme unverzichtbare Infrastruktur darstellen.

Dr. Carsten Ulbricht ist auf Internet und die digitale Transformation spezialisierter Rechtsanwalt bei der Stuttgarter Kanzlei Menold Bezler mit den Schwerpunkten Internet- und IT-Recht sowie Datenschutz. Im Rahmen seiner anwaltlichen Tätigkeit berät Dr. Ulbricht nationale und internationale Mandanten in allen Rechtsfragen des E- und Mobile Commerce, Big Data, sowie zu allen Themen im Bereich Social Media. Neben seiner Referententätigkeit berichtet er seit dem Jahr 2007 regelmäßig in seinem Weblog zum Thema »Internet, Social Media & Recht« unter www.rechtzweinull.de nicht nur über neueste Entwicklungen in Rechtsprechung, Diskussionen in der Literatur und über eigene Erfahrungen, sondern analysiert auch digitale Projekte auf ihre rechtlichen Erfolgs- und Risikofaktoren. In seinem Buch »Social Media & Recht – Praxiswissen für Unternehmen« fasst Dr. Ulbricht die wichtigsten rechtlichen Fragen zusammen.

Anna Deckert leitet in der Kommunikationsbüro Ulmer GmbH den Bereich Bildung für Nachhaltige Entwicklung und Transformation. Sie unterstützt Ministerien, Kommunen und Unternehmen bei der Strategieentwicklung, Stakeholderbeteiligung, Vernetzung und Umsetzung innovativer Veranstaltungsformate. Gleichzeitig ist Sie bei DIALOGIK tätig und erprobt dort neue Ansätze für Bürgerbeteiligung, Leitlinien und die Verstetigung von Engagement.



Kontakt

Kommunikationsbüro Ulmer GmbH
Frank Ulmer
Teckstraße 56
70190 Stuttgart
Tel.: 0711 259 717 20
post@kommunikationsbuero.com

Redaktion eNewsletter

Netzwerk Bürgerbeteiligung
c/o Stiftung Mitarbeit
Redaktion eNewsletter
Ellerstraße 67
53119 Bonn
E-Mail: newsletter@netzwerk-buergerbeteiligung.de