Tipps zum Umgang mit Datenschutz bei Kollaborationstools

Ein Leitfaden erstellt für den Paritätischen Wohlfahrtsverband

Von Dr. Olaf Koglin

#gleich im Netz

DER PARITÄTISCHE GESAMTVERBAND

Inhalt

Teil 1: Tools und Themen: Worum geht es bei Kollaboration? 5

Teil 2: Was ist Datenschutz? 9

Teil 3: Checkliste für den Einsatz von Kollaborationstools 21

Teil 4: Zwei konkrete Beispiele 27

Teil 5: Do‘s & Don‘ts und häufig gestellte Fragen 31

Teil 6: Anhang 39

Einleitung

Mit den Lockdown-Phasen der Corona-Zeit gab es zwei große Gewinner: Online-Shops und Anbieter für die digitale Zusammenarbeit. So hatte im Frühjahr 2020 der Aktienkurs von Zoom Technologies ein Plus von fast 900% erreicht – bis die Anleger*innen bemerkten, dass sie die Papiere einer ganz anderen Firma mit dem Namen „Zoom" gekauft hatten (bit.ly/Paritaet-ZoomAktie).

Datenschutz ist in der digitalisierten Gesellschaft ein zentrales Grundrecht und elementar wichtig. Im Arbeitsumfeld vereint es den Schutz von Persönlichkeit und Privatsphäre einer*s jeden Einzelnen mit dem, was im produzierenden Gewerbe Aufgabe des Arbeitsschutzes war: Für sichere und rechtskonforme Arbeitsmittel und Arbeitsumfelder zu sorgen.

Gleichzeitig verlangen Digitalisierung, Innovation und agiles Arbeiten, auf Neuerungen und Veränderungen schnell zu reagieren. Die Nutzung neuer Software setzt dank der Cloud nicht langwierige Ausschreibungen, Lizenzverhandlungen und neue Server voraus, sondern einen Klick auf der Website des Anbieters. Wenn das Software as a Service-Angebot wie so oft kostenlos nutzbar ist, bekommt der Arbeitgeber häufig gar nicht mit, welche Daten der*die Mitarbeiter*in in welchem Land verarbeiten lässt. Da im Wesen von Kommunikation liegt, dass andere beteiligt sind, wird einem leider auch häufig die Entscheidung über ein Tool vorgegeben: Wer hat es noch nicht erlebt, dass Geschäftspartner für die wichtige Videokonferenz einen Link zu einem Anbieter senden, den man noch nicht kennt, das Dokument dazu wie selbstverständlich „in der Cloud geshared" wird oder im Sportverein wichtige Planungen nur über WhatsApp oder Facebook laufen?

Die 18 deutschen Aufsichtsbehörden haben inzwischen eine unüberschaubare Anzahl von Empfehlungen veröffentlicht, die leider vor allem eines eint: Sie helfen kaum, beziehen sich oft auf veraltete Versionen, säen Bedenken und raten ab, oder geben praxisferne Tipps, wie etwa die Software auf eigenen Servern zu hosten. So kann man Deutschland nicht digitalisieren.

Dieser Leitfaden will einen Mittelweg finden: Datenschutz ist dem Paritätischen und seinen Mitgliedern ein wichtiges Anliegen. In der Realität kann aber von einem kleinen Verein nicht für jede testweise Nutzung eines neuen Cloud-Tools eine umfangreiche Datenschutzprüfung nebst IT-Sicherheitsaudit und Verhandlung von Verträgen und zusätzlichen Garantien mit einem US-Anbieter durchgeführt werden. Ganz häufig werden Sie in der Praxis zwischen einem „das Tool nutzen doch alle" und einem „aber eigentlich gibt es Bedenken" stehen. Als praxisnaher Leitfaden wollen wir Sie zu verantwortlichem Handeln befähigen, bei dem wirkliche Risiken nicht ignoriert, aber theoretische Probleme auch nicht zum permanenten Verhinderer werden. Die jeweilige Risikoentscheidung kann Ihnen weder vom Paritätischen Gesamtverband noch von Anwälten abgenommen werden.

TEIL 1

Tools und Themen: Worum geht es bei Kollaboration?

Kollaborationstools, oder frei übersetzt Software für die digitale Zusammenarbeit, gehören zu den großen Gewinnern der Corona-Krise. Zwar existieren Elemente davon – wie Skype oder Chat-Funktionen – zum Teil schon seit Jahrzehnten. Aber in der derzeitigen Funktionsvielfalt und unter diesem Titel haben sie für die breite Masse der Beschäftigten erst durch „Home Office“ alltägliche Bedeutung erlangt.

Im Kern geht es bei Kollaborationstools darum,

- die als veraltet und umständlich empfundene Kommunikation über E-Mail, Telefon oder gar Telefax durch moderne Techniken abzulösen **(Digitalisierung)**: Slack wirbt in Deutschland mit dem Slogan „Wie arbeiten, nur besser",
- schnellere Mittel für Textkommunikation (wie Messenger) zu nutzen und Video- und Audio-Kommunikationsmittel zur Verfügung zu stellen, die auch mit mehreren Teilnehmer*innen und Zusatzfunktionen wie dem Teilen des Bildschirmes unkompliziert genutzt werden können **(Kommunikation)**,
- eine gemeinsame Übersicht über Dokumente und Aufgaben zu haben und diese gemeinsam bearbeiten zu können **(Zusammenarbeit)**, und
- diese Funktionen nicht nur stationär an einem Endgerät nutzen zu können, sondern von jedem Rechner, Tablet oder Smartphone aus jederzeit darauf zugreifen zu können **(Mobilität)**. Dies wird oft durch den Slogan „Arbeite wo und wann Du willst" ausgedrückt; die wichtige soziale und arbeitsrechtliche Thematik der Entgrenzung von Arbeit und Privatleben wird in diesem datenschutzrechtlichen Leitfaden außen vor gelassen.

Unter dem Begriff der Kollaborationstools wird damit eine breite Palette von Funktionen und Anbietern zusammengefasst. Diese lassen sich in fünf Kategorien einteilen:

1. **Messaging- und Kommunikationsfunktionen**
2. **Video- und Konferenzsysteme**
3. **File Sharing und gemeinsame Dokumentenbearbeitung**
4. **Task Management**
5. **Sonstige**, wie zur **Moderation** und Durchführung von **Workshops**, Teilnehmer-**Feedback**, Zusatzfunktionen für einzelne Dienste (z.B. Adressbuch), **Automatisierung** oder die Übersicht über die Kommunikation in den eingesetzten Kollaborationstools.

Eine ausführliche Auflistung aktueller Tools findet sich in der Übersicht im Webzeugkoffer des Paritätischen www.der-paritaetische.de/webzeugkoffer (Abdruck siehe letzte Seite 40-41).

Die Darstellung als Marktübersicht nach Funktionen und Anbietern wird dadurch erschwert, dass die Tools typischerweise mehrere Funktionen verbinden, um Nutzer*innen die Nutzung so einfach wie möglich zu machen (und um zu vermeiden, dass sie wegen fehlender Funktionen zu anderen Tools wechseln). So sind zum Beispiel Slack und WhatsApp im Kern Messaging- und Textkommunikationstools, verfügen aber inzwischen auch über Funktionen zum Video- oder Audioanruf. Umgekehrt haben die klassischen Videokonferenz-Tools (wie Skype und zoom) auch immer Chatfunktionen und meist auch die Möglichkeit zum „Teilen" von Dokumenten, also Dienste aus den Kategorien „Messaging" und „File Sharing".

Dass solche zusätzlichen Produktfunktionen („Features") recht häufig und schnell integriert werden, liegt auch daran, dass die Komponenten selbst (wie Chat-Funktionen oder Videotelefonie) in der Regel keine „Rocket Science" darstellen, sondern seit langem erprobt und verfügbar sind – Skype wurde 2003 gegründet. Die Herausforderung und Innovation seitens der Anbieter liegt eher in der Performance und vor allem einer guten „User Experience", also Benutzbarkeit und intuitiver Anwendbarkeit. Folglich können gefragte Funktionen auch schnell implementiert werden: Zu Beginn des Corona-Lockdowns im März 2020 ermöglichte Zoom einen künstlichen Hintergrund, was Teams-Nutzern damals noch nicht möglich war. Doch Microsoft zog alsbald nach.

So wird es sicherlich weitergehen: In einem Jahr sehen die Tools ganz anders aus als heute, und in fünf Jahren haben wir wiederum völlig neue Tools und Arbeitsweisen.

Kollaborationstools und ihre Funktionen

1. Messaging- und Kommunikationsfunktionen

Für geschäftliche Zwecke: Slack, Teams - Open Source-Alternativen: Mattermost, Rocketchat.
Für private Zwecke und mit weniger Funktionen: WhatsApp, Signal, Threema und die in anderen sozialen Medien enthaltenen Messenger (u.a. Facebook Messenger, Instagram, SnapChat).

2. Video- und Konferenzsysteme

Beispiele: Zoom, Teams, Skype, Google Hangouts, WebEx, GoToMeeting, BlueJeans.
Open Source: jitsi Meet oder BigBlueButton, die entweder selbst gehostet oder von Dienstleistern als Service genutzt werden können.

3. File Sharing und gemeinsame Dokumentenbearbeitung

Beispiele: GoogleDocs, Microsoft Sharepoint.
Für Notizen/Protokolle: Microsoft OneNote.
Als Open Source Software: Etherpad, als Service z.B. bei pad.systemli.org

4. Task Management

Im Stil einer Kanban-Board-Ansicht: Trello, Microsoft Planner, MeisterTask.
Open Source: Wekan.
Je nach Arbeitsweise auch als Projekt- und Zeitübersicht (Asana), Ticket-Systeme (ServiceNow, Jira) oder reine ToDo-Listen (u.a. Microsoft To Do und Lists).

5. Sonstige, wie

- Unterstützung und Visualisierung bei moderierten Meetings. Beispiel: Miro, eine Mischung aus Brainstorming, digitalen Post-Its nebst „Mapping“ und mehr
- Zusatzfunktionen für bestehende Dienste (z.B. Adressbuch).
- Weiterleiten / Upload von Dateien (z.B. wetransfer).
- Präsentationen jenseits von PowerPoint (z.B. prezi, Pitch).
- Präsentations- und Visualisierungstools, z.B. Whiteboards, Teilnehmerumfragen, sog. Wortwolken.
- Übersicht und Zusammenführung von gleichzeitig genutzten Kollaborationstools und der eingehenden Nachrichten. Beispiel: BaaS.
- Automatisierung von Abläufen und Funktionen über mehrere Tools (z.B. Microsoft Power Automate [ehemals „Flow“], IfThisThenThat).

DSGVO
Goals
Teamwork
Customers
Costs
Income
Plan

TEIL 2

Was ist Datenschutz?

Datenschutz bedeutet zunächst, unabhängig von gesetzlichen Pflichten oder Bußgeldern **verantwortungsbewusst** mit Informationen umzugehen, und gehört zum Selbstverständnis der sozialen Arbeit. Die konkreten Pflichten entstehen durch das Datenschutz-Recht, wozu in der EU vor allem die DSGVO gehört.

1. Hat die DSGVO alles verändert?

Spätestens seit Geltung der **EU-Datenschutz-Grundverordnung (DSGVO)** im Mai 2018 ist Datenschutz allgegenwärtig – und nicht immer beliebt, wird „der Datenschutz" doch häufig als Verhinderer dargestellt, der Fotos der Kita-Gruppe, Online-Unterricht während der Corona-Zeit oder die Digitalisierung im Allgemeinen vereitelt.

Dabei gab es die meisten Regelungen der DSGVO bereits vorher in der europäischen Datenschutz-Richtlinie aus 1995 (95/46/EG), die – anders als eine EU-Verordnung – durch die Mitgliedsstaaten erst noch in nationales Recht umgesetzt werden musste. Man kann also sagen, dass die gleichen Regeln, die über 20 Jahre lang nur wenig beachtet wurden, durch die mit der DSGVO und ihre Bußgelder einhergegangene Berichterstattung erst wirklich relevant wurden.

Ein generelles Problem bei der DSGVO ist, dass es viele unklare Begriffe und recht wenige Gerichtsurteile zu ihr gibt. Dadurch gibt es zu vielen Interpretationsfragen leider immer noch keine klaren Antworten. Doch mit der Digitalisierung kann nicht gewartet werden, bis auch die letzte Frage vom Europäischen Gerichtshof geklärt wurde.

Die DSGVO verwendet folgende Begriffe:

Die Organisation, die die Daten verarbeitet, wird **„Verantwortlicher"** genannt. Dies ist meist der e.V., die Stiftung oder gGmbH, dem*der umgangssprachlich die Daten „gehören". Genau genommen ist es aber der*diejenige, der „über die Zwecke und Mittel" der Datenverarbeitung entscheidet (Art. 4 Nr. 7 DSGVO). Dies können evtl. sogar zwei Organisationen gemeinsam sein (Art. 26 DSGVO).

Der*die **„Betroffene"** ist die Person, um die es in den Daten geht, z.B. in der Mitgliederliste eines e.V. oder als Teilnehmer in einer Videokonferenz (Art. 4 Nr. 1 DSGVO).

Einen **„Eigentümer"** der Daten gibt es im Datenschutz nicht. Der*die Betroffene wird durch die DSGVO geschützt, und der Verantwortliche verantwortet die Datenverarbeitung und die Einhaltung der DSGVO (Art. 5 DSGVO).

2. Wann gilt die DSGVO – oder: Was sind personenbezogene Daten?

Wichtig: Die DSGVO gilt nur für **„personenbezogene Daten"**. Dies sind nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf einen identifizierten oder identifizierbaren lebenden Menschen beziehen. Es reicht aus, wenn die Person erst durch weitere Informationen identifiziert werden kann. Personalnummern oder Kfz-Kennzeichen gelten daher schnell als „personenbezogene Daten". Ungeklärt ist, wie viel Aufwand, Zusatzwissen oder gar kriminelle Energie unterstellt werden muss, um zu bewerten, ob bestimmte Daten personenbezogen sind. In der Praxis werden angesichts der Rechtsprechung von EuGH und BGH meist sogar Cookies und IP-Adressen als personenbezogene Daten angesehen (bit.ly/Parita-et-Breyer). Auf jeden Fall sind in der Praxis in Kollaborationstools immer personenbezogene Daten enthalten, da User sich anmelden und Informationen eingeben, die mit ihnen selbst oder mit anderen Menschen im Zusammenhang stehen.

Die Regelungen der DSGVO gelten für jede Form der Datenverarbeitung. Eine **„Verarbeitung"** liegt nach der Definition des Art. 4 Nr. 2 DSGVO auch schon dann vor, wenn die Daten gar nicht klassisch gespeichert werden: Auch die Übermittlung der Daten und die bloße Bereitstellung zum Zugriff stellen nach Art. 4 Nr. 2 DSGVO eine Verarbeitung dar, für die es einer Rechtsgrundlage bedarf. Die bloße Übertragung einer identifizierbaren Person im Video-Chat unterliegt daher den Anforderungen der DSGVO; zu beiläufigen Gesundheitsdaten dabei siehe unten Ziff. 5.

Die **rein private Datenverarbeitung** unterliegt übrigens nicht der DSGVO. Deren Anwendungsbereich ist nach Art. 2 Abs. 2 (c) DSGVO auf die Verarbeitung durch natürliche Personen zu ausschließlich persönlichen oder familiären Tätigkeiten beschränkt. Die Grenzen dafür werden vom EuGH sehr eng gezogen, d.h. bei einer für viele Teilnehmer offenen Zoom-Party, einem großen Adressbuch, das zu WhatsApp hochgeladen wird, oder Videoaufnahmen außerhalb des eigenen Grundstücks

hat man diese Ausnahme schnell verlassen und ist im Anwendungsbereich der DSGVO. Auch kann ein Arbeitgeber nicht anweisen, dass Mitarbeiter*innen an einem dienstlichen WhatsApp-Chat teilnehmen müssen und dies zugleich als private Aktivität deklarieren, die nicht der DSGVO unterliege.

Merke:

- Datenschutzrecht gilt nur, wenn es sich um personenbezogene Daten handelt – und das ist bei Kollaborationstools praktisch immer der Fall.
- Auch Aufnahmen von erkennbaren Personen, egal ob per Überwachungskamera oder per Videokonferenz, können als „personenbezogene Daten" gelten.
- Rein private Aktivitäten unterliegen nicht der DSGVO. Diese Ausnahme ist aber sehr eng begrenzt.

3. Die DSGVO regelt sowohl die Datennutzung als auch die Datenschutz-Bürokratie

Die für die Praxis relevanten Regelungen der DSGVO lassen sich grob in zwei Bereiche aufteilen: Die operative Frage, welche Daten auf welcher Rechtsgrundlage zu welchem Zweck verwendet werden dürfen, und die administrative Frage, was dafür an Bürokratie erforderlich ist. Hierzu gehören z.B. Datenschutzerklärungen, Dokumentationen und Löschkonzepte; siehe Ziff. 6 und Teil 3 Ziff. 5.

4. Was sind die Voraussetzungen, Daten nutzen zu dürfen?

Unter der DSGVO dürfen personenbezogene Daten nur verarbeitet werden, wenn der Datenverarbeiter (der „Verantwortliche") eine Rechtsgrundlage hierfür hat. Die möglichen Rechtsgrundlagen sind in Art. 6 Abs. 1 DSGVO definiert. Die für die Praxis Relevanten sind: Einwilligung, Berechtigtes Interesse, gesetzliche Pflicht, Vertrag.

Als **Vertrag** gilt auch der Arbeitsvertrag zwischen Mitarbeiter*in und Arbeitgeber. Im Beschäftigten-Datenschutz kommt eine Zusatznorm hinzu: Über Art. 88 DSGVO durfte Deutschland mit § 26 BDSG eine abweichende Rechtsgrundlage erlassen. Danach dürfen Daten für die Durchführung des Beschäftigungsverhältnisses verarbeitet werden, und um Rechte und Pflichten aus einer Betriebsvereinbarung umzusetzen (auch durch den Betriebsrat).

Die **gesetzliche Pflicht** ist als Rechtsgrundlage u.a. bei der Gehaltsabrechnung und den Meldepflichten an Finanzämter und Sozialversicherungsträger relevant, spielt für Kollaborationstools aber keine Rolle.

Einwilligung (teilweise auch Opt-In genannt)

Beschreibung: Der*die Betroffene erklärt aktiv, mit der Verarbeitung der Daten einverstanden zu sein. Dies kann durch Ankreuzen/Anklicken eines Auswahlfeldes erfolgen oder durch klicken auf ein Feld, das „Einverstanden" oder ähnlich benannt ist.
Vorteil: Die Einwilligung kann eingeholt werden, wenn die anderen Rechtsgrundlagen nicht greifen oder wenn sie zwingend erforderlich ist (Art. 9 DSGVO).
Nachteil: Es gibt sehr hohe und unklare Anforderungen an die vorherige Informiertheit der Betroffenen, Transparenz, Freiwilligkeit und vieles mehr. Dies ist zumindest bei komplexen Datenverarbeitungen schwer einzuhalten.
Die Einwilligung ist jederzeit widerrufbar.

Bei Arbeitnehmer*innen ist eine Einwilligung gegenüber dem Arbeitgeber fast nie durchsetzbar, da die Gerichte die Freiwilligkeit verneinen. Jedenfalls können Arbeitgeber ihre Mitarbeiter*innen nicht dazu zwingen, „freiwillig" eine Einwilligung zur Nutzung bestimmter Kollaborationstools zu erteilen. Bei Arbeitnehmer*innen wird als Rechtsgrundlage meist auf den Vertrag, eine Betriebsvereinbarung oder ein Berechtigtes Interesse zurückgegriffen.

Berechtigtes Interesse

Beschreibung: Abwägung zwischen den vernünftigen Interessen des Verantwortlichen an der Verarbeitung und dem Risiko, das dadurch für die Betroffenen entsteht.
Vorteil: Fast immer anwendbar (außer Art. 9); Widerspruchsrecht nur begrenzt.
Nachteil: Als Abwägung subjektiv und damit angreifbar: Wer die Argumente anders gewichtet, kann zu einem anderen Ergebnis kommen.

Das Berechtigte Interesse ist zu dokumentieren. Die Betroffenen sind über das Berechtigte Interesse sowie über ihr Widerspruchsrecht zu informieren, was häufig nicht akkurat umgesetzt wird (Art. 13 Abs. 1 (d), 21 Abs. 4 DSGVO; zu Einschränkungen des Widerspruchsrechts Art. 21 Abs. 1 S. 2 DSGVO).

Vertrag oder Vertragsvorbereitung

Beschreibung: Es reicht ein **Vertrag mit dem/der Betroffenen**; Entgeltlichkeit ist nicht erforderlich. Auch die Vertragsvorbereitung (sofern sie vom Betroffenen ausgeht) und -beendigung sind erfasst. Die Rechtsgrundlage ist auf die Tätigkeiten beschränkt, die für die Umsetzung des Vertrags **erforderlich** sind.
Vorteil: Es sind keine weiteren Formalitäten erforderlich. Kein Widerrufs- oder Widerspruchsrecht.
Nachteil: Der Vertrag muss zwischen dem Verantwortlichen **und der betroffenen Person** geschlossen werden.

Achtung: Bei einem Vertrag zwischen Dienstleister und Arbeitgeber ist der*die Mitarbeiter*in nicht Vertragspartei.

*Beispiel: Der Arbeitgeber hat einen Vertrag mit einem Anbieter von Software zur Gehaltsabrechnung geschlossen. Dieser Vertrag ist im Verhältnis zu den Mitarbeiter*innen keine Rechtsgrundlage, um deren Gehaltsdaten zu verarbeiten.*

Das Gleiche gilt bei Verträgen mit Anbietern von Kollaborationstools: Der vom Arbeitgeber abgeschlossene Vertrag kann nicht als Rechtsgrundlage für die Datenverarbeitung herhalten.

Betriebsvereinbarung

Beschreibung: Unterform der Rechtsgrundlage „Vertrag"; vgl. Art. 88 DSGVO, § 26 BDSG.
Vorteil: Bei Vorliegen einer entsprechenden Betriebsvereinbarung eine **sichere Rechtsgrundlage**.
Nachteil: Abschluss einer BV erforderlich, die diese Art der Datenverarbeitung explizit regelt. Gilt nur ggü. Beschäftigten, nicht ggü. freien Mitarbeiter*innen oder Dritten. Betriebsvereinbarungen sind meist aufwändig und statisch, daher begrenzt für das agile Arbeiten mit immer wieder neuen Diensten einsetzbar.

Achtung: Wegen des Geltungsbereichs des Betriebsverfassungsgesetzes (BetrVerfG) dient eine Betriebsvereinbarung nur innerhalb von Deutschland als Rechtsgrundlage und nur für die Personen, die gem. **§ 5 BetrVerfG als „Arbeitnehmer"** gelten – nicht dazu gehören Vorstände/Geschäftsführer sowie Personen, die aus karitativen bzw. religiösen Beweggründen oder zur Wiedereingewöhnung beschäftigt sind.

Wichtig für Vereine:
Die Datenschutzbehörden erkennen an, dass eine Vereinsmitgliedschaft als „Vertrag" i.S.d. Art. 6 Abs. 1 (b) DSGVO gilt. Somit kann das, was für die **Verwaltung der Mitgliedschaft** erforderlich ist, auf diese Rechtsgrundlage gestützt werden. Die Kommunikation per Slack oder anderen Kollaborationstools wird aber nach den strengen Auffassungen der Aufsichtsbehörden hierfür nicht zwingend erforderlich sein, in diesen Fällen kann ggf. auf ein berechtigtes Interesse zurückgegriffen werden (bit.ly/Paritaet-eV).

Wichtig für Verträge bei Vereinen:
Achtung: Der (Mitglieds-) Vertrag einer Mitgliedsorganisation mit einem Landesverband oder mit dem Bundesverband ist kein Vertrag der Mitarbeiter*innen oder der Vereinsmitglieder. Für die Weitergabe von ihren Daten können in bestimmten Fällen andere Rechtsgrundlagen herangezogen werden, z.B. der Arbeitsvertrag der Mitarbeiter*innen oder ein Berechtigtes Interesse.

5. Besonderheiten bei Kindern und bei sensiblen Daten

Bei Kindern unter 16 Jahren muss die Einwilligung von den Erziehungsberechtigten kommen (Art. 8 DSGVO).
Art. 9 DSGVO setzt sehr strenge Anforderungen für die Verarbeitung besonders sensibler Daten. Diese dürfen meist nur mit ausdrücklicher Einwilligung des Betroffenen verarbeitet werden.

Was sind sensible Daten nach Art. 9 DSGVO?

Dies sind personenbezogene Daten, aus denen die **„rassische und ethnische** Herkunft, **politische Meinungen, religiöse** oder weltanschauliche Überzeugungen oder eine **Gewerkschaftszugehörigkeit** hervorgehen," sowie **genetische und biometrische Daten, Gesundheitsdaten** oder Daten zum Sexualleben oder der **sexuellen Orientierung**.

Dies klingt zunächst vernünftig, da diese Daten und die Personen dahinter besonders schützenswert sind. Da aber schon eine Brille auf eine Sehschwäche schließen lässt und daher als Gesundheitsdatum gilt, liegen bei harmlosen Videokonferenzen schnell als unbeabsichtigter „Beifang" einige Gesundheitsdaten vor. Gleiches gilt für das Tragen eines Kreuzes oder einer Burka (religiöse Überzeugung) oder eines Regenbogen-Ansteckers (sexuelle Orientierung). Daher haben erste Gerichte entschieden, dass die Restriktionen des Art. 9 DSGVO nicht anwendbar sind, wenn der Verantwortliche keine Auswertungsabsicht in Bezug auf die sensiblen Daten hat (VG Mainz, Urteil vom 24.9.2020 – bit.ly/Paritaet-VG). Eine „normale" Rechtsgrundlage aus Art. 6 DSGVO muss natürlich trotzdem vorliegen.

6. Datenschutz-Bürokratie

Zusätzlich zu den teils anspruchsvollen Anforderungen an die Rechtsgrundlagen müssen noch allgemeine datenschutzrechtliche Anforderungen beachtet werden. Neben den Grundlagen einer Datenschutz-Organisation (u.a. Art. 5 Abs. 2 DSGVO: Rechenschaftspflicht) kann hierzu insbesondere gehören, vorab eine sog. Datenschutz-Folgenabschätzung durchzuführen (Art. 35 DSGVO) und das Kollaborationstool vollständig in das Verarbeitungsverzeichnis (Art. 30 DSGVO) aufzunehmen. Zudem sind ggf. Informationen über das Widerrufs- bzw. Widerspruchsrecht und die Pflichtinformationen nach Art. 13, 14 DSGVO zu erteilen, ganz zu schweigen von technischen und organisatorischen Maßnahmen sowie der Benennung eines Datenschutzbeauftragten. Vgl. dazu Teil 3 Ziff. 5 (Checkliste) und zu allgemeinen Anforderungen das Heft „Erste Hilfe zur DSGVO".

Hinzuweisen ist auch darauf, dass gesetzliche Anforderungen wie die **Umsetzung eines Löschkonzepts** und ggf. gesetzliche Aufbewahrungspflichten auch bei Kollaborationstools gelten. Dies kann vor allem dann anspruchsvoll sein, wenn Mitarbeiter*innen im Rahmen des „Bring Your Own Device" (BYOD) Privatgeräte einsetzen, um die Daten der Organisation auf dem Smartphone zu nutzen.

7. Was ist beim Einsatz von Dienstleistern zu beachten, und was meint „AVV“?

Wenn ein Unternehmen oder eine Organisation „seine“ Daten durch einen Dienstleister verarbeiten lässt, wäre dies eine „Übermittlung“ (Art. 4 Nr. 2 DSGVO) an Dritte. Schon für diese Übermittlung ist – abgesehen von der eigentlichen Datenverarbeitung und der dafür erforderlichen Rechtsgrundlage – eine eigene Rechtsgrundlage erforderlich.

Die Konstruktion der **Auftragsverarbeitung** will dies vereinfachen. Sofern der Dienstleister als „verlängerte Werkbank“ die Daten weisungsgebunden im Auftrag des Verantwortlichen verarbeitet (daher der Name „Auftragsverarbeitung“) und er die Daten getrennt von den Daten anderer Kunden und seiner eigenen Daten hält, gilt er nicht als Dritter, sondern sozusagen als Teil des Auftraggebers. Der Preis dafür sind die Weisungsgebundenheit und die Pflicht, nach Art. 28 DSGVO eine sehr ausführliche Vereinbarung über die Auftragsverarbeitung abzuschließen. Diese Auftragsverarbeitungs-Vereinbarung wie auch die Auftragsverarbeitung selbst wird AVV abgekürzt, in englischen Dokumenten DPA (Data Processing Agreement). Die AVV ist meist ein sehr langes Dokument mit Anlagen zur Beschreibung der Datenverarbeitung, der IT-Sicherheitsmaßnahmen des Dienstleisters (TOMs) und der zugelassenen Subunternehmer. Dadurch erscheint sie als sehr lästige Pflicht. In Wahrheit ist sie aber eine Vereinfachung (wie Juristen sagen: eine Privilegierung), dank derer der Dienstleister nicht als Dritter gilt.

Die in Art. 28 DSGVO vorgesehene Pflicht zur Überprüfung der TOMs und auch der Subunternehmer bereiten in der Praxis oft Probleme oder werden vernachlässigt.
Gegenstücke zur AVV sind die Joint Controller-Vereinbarung (Art. 26 DSGVO) und die Controller-to-Controller-Vereinbarung, die bei Kollaborationstools keine so große Rolle spielen.

Wer sind Dritte?

Die DSGVO kennt kein „Konzernprivileg“: Jede rechtliche Organisationseinheit ist in der Regel ein eigener „Verantwortlicher“ und jeder andere ein Dritter, sofern keine AVV vorliegt. Dies gilt auch zwischen einer gGmbH und der von ihr gegründeten Service-GmbH oder zwischen einem e.V. und einer gGmbH, deren Alleingesellschafter der e.V. ist.
Das heißt: Die personenbezogenen Daten können nicht einfach zwischen den Organisationen ausgetauscht werden, sondern es bedarf einer Rechtsgrundlage für die Übermittlung oder einer AVV.

8. Max Schrems, CLOUD Act und der EuGH: Dienstleister und Datenübertragung außerhalb der EU

Achtung – Fristen für die neuen SCC:
Die EU-Kommission hat im Sommer 2021 neue Standardvertragsklauseln (SCC) zur Verfügung gestellt. **Seit 27.09.2021 dürfen für neu abzuschließende Verträge** nur noch diese neuen SCC-Fassungen verwendet werden. **Bis zum 27.12.2022 müssen auch alle Bestandsverträge** auf die neuen SCC umgestellt worden sein.

Innerhalb der EU wird durch die DSGVO und das weitere EU-Recht davon ausgegangen, dass überall ein hohes und vergleichbares Schutzniveau für personenbezogene Daten herrscht. Daher darf ein Verantwortlicher all das, was er in Deutschland darf, auch innerhalb der EU umsetzen. Dabei spielt es keine Rolle, ob er die Daten selbst verarbeitet oder dies durch Dienstleister erbringen lässt, z.B. im Rahmen der AVV.

Durch Dienstleister außerhalb der EU ist dies nur zulässig, wenn bei diesen ein sog. **„angemessenes Schutzniveau"** vorliegt, also ein vergleichbar hoher Datenschutz wie in der EU gegeben ist (Art. 44, 45 DSGVO). Dies kann entweder grundsätzlich für ein Land gegeben sein oder aber nur für einzelne Unternehmen, selbst wenn deren Land als solches keinen ausreichenden Schutz aufweist, aber das Unternehmen besondere (und wirksame) Garantien gibt. Für die nicht zur EU gehörenden Länder des Europäischen Wirtschaftsraums (EWR) wurde dieses Schutzniveau anerkannt (Island, Norwegen und Liechtenstein). Auch für einige andere Länder wurde das Schutzniveau von der EU anerkannt (u.a. Japan, Israel und mit Einschränkungen Kanada). Die USA sind jedoch nicht dabei – was seit Jahrzehnten zu Schwierigkeiten führt.

Der österreichische Jurist und Datenschutz-Aktivist **Max Schrems** hat als Student zunächst das sog. „Safe Harbor"-Abkommen zwischen der EU und den USA vor dem EuGH zu Fall gebracht. Anschließend hat er auch gegen die Nachfolgeregelung „EU-U.S. Privacy Shield" geklagt – und vor dem EuGH erneut gewonnen. Dies steht auch vor dem sehr politischen Hintergrund der Snowden-Enthüllungen zur Massenüberwachung durch US-Dienste sowie dem US-amerikanischen CLOUD Act, der US-Unternehmen verpflichtet, auch außerhalb der USA gespeicherte Daten an US-Behörden herauszugeben.
Für Cloud-Services praxisrelevant sind damit nicht mehr das Privacy Shield, sondern nur noch die sog. Standardvertragsklauseln der EU (auch EU Model Clauses oder Standard Contractual Clauses, SCC). Dies sind Musterverträge der EU-Kommission aus, mit denen der Datenschutz beim Dienstleister vertraglich auf EU-Niveau gehoben werden sollte. In der Praxis wurden sie häufig blind von Auftraggeber und Auftragnehmer unterschrieben, um formal den Anforderungen an Datentransfers in Drittstaaten zu genügen. Selbstverständlich hilft dies nicht gegen Kernfragen wie die Zugriffsmöglichkeiten von US-Behörden. Vor dem Hintergrund der „Schrems II"-Entscheidung des EuGH hat die EU-Kommission im Juni 2021 neue Fassungen der Standardvertragsklauseln (SCC) beschlossen (bit.ly/Paritaet-SCC). Im Gegensatz zu den bisherigen Fassungen aus 2001 und 2010 sind diese modular aufgebaut: Es gibt als Rahmen einen Haupttext, aber einzelne Ziffern (die hier „Klauseln" heißen) sind abhängig davon einzusetzen, welche Version der SCC gewünscht ist. „Modul Zwei" ist die Version für die Übermittlung von Verantwortlichen an Auftragsverarbeiter, also die häufig verwendete Variante für AVV-ähnliche Sachverhalte.
Der Auftraggeber muss hiernach die Rechtslage im Zielland beurteilen und sich geeignete Garantien einräumen lassen. Dies erscheint für kleinere Vereine wenig realistisch und wird unter dem Begriff Transfer Impact Assessment (TIA; auch: Data Transfer Impact Assessment / DTIA) zusammengefasst.
Seit 27.09.2021 dürfen für neu abzuschließende Verträge nur noch diese neuen SCC-Fassungen verwendet werden. **Bis zum 27.12.2022 müssen auch alle Bestandsverträge** auf die neuen SCC umgestellt worden sein.

Dem **CLOUD Act** war ein jahrelanger Rechtsstreit zwischen Microsoft und US-Behörden vorangegangen. Diese hatten von Microsoft die Herausgabe von in Irland gespeicherten Daten verlangt, wogegen Microsoft sich in mehreren Instanzen bis zum Supreme Court wehrte. Mit dem 2018 erlassenen "Clarifying Lawful Overseas Use of Data Act" (kurz CLOUD Act) wurde eine Entscheidung zur alten Rechtslage obsolet. Unter dem CLOUD Act kann von US-amerikanischen Gesellschaften die Herausgabe der Daten von Nicht-US-Bürgern verlangt werden, auch wenn diese außerhalb der USA gespeichert werden. Diese „extraterritoriale Wirkung" eines US-Gesetzes ist bei Bürgerrechtlern und Datenschützern auf starke Kritik gestoßen, da üblicherweise ein Rechtshilfeersuchen zu stellen wäre, bei dem i.d.R. ein Gericht aus dem betreffenden Land eine Überprüfung des Ersuchens vornehmen kann (vgl. Art. 48 DSGVO). Mangelnde Garantien für den Schutz der Daten von EU-Bürgern waren auch ein zentrales Argument des EuGH bei seiner Entscheidung, das „Privacy Shield" für ungültig zu erklären („Schrems II").

Der EuGH hat in der „Schrems II"-Entscheidung über die Fragen zum Privacy Shield hinaus entschieden, dass der reine Abschluss der Standardvertragsklauseln nicht ausreicht, sondern der Dienstleister auch tatsächlich Garantien für die Datensicherheit zu bieten hat, und der Auftraggeber diese zu überprüfen hat.

9. Wie soll man mit der Unsicherheit und den Positionen der Aufsichtsbehörden umgehen?

Im Anschluss an die „Schrems II"-Entscheidung des EuGH hat im November 2020 der Europäische Datenschutz-Ausschuss, eine Art Zusammenschluss der europäischen Aufsichtsbehörden, Richtlinien für die Prüfung entsprechender Garantien vorgeschlagen. Wie bei allen Stellungnahmen von Aufsichtsbehörden ist festzuhalten, dass es sich dabei nicht um Gesetze oder zwingendes Recht handelt, sondern „nur" um eine Rechtsauffassung – allerdings um eine sehr erhebliche, weil die Behörden oft entsprechend vorgehen werden.

Die Aufsichtsbehörden raten angesichts der beschriebenen Rechtslage davon ab, überhaupt Dienstleister aus den USA einzusetzen – jedenfalls sofern mit diesen keine zusätzlichen Garantien vereinbart wurden. Die Aufsichtsbehörden raten übrigens auch davon ab, übliche (unverschlüsselte) E-Mails oder Telefaxe zu versenden, Windows10 zu verwenden und schlagen grundsätzlich vor, Software nicht aus der Cloud zu nutzen, sondern sie selbst – möglichst als Open Source Software – auf eigenen Servern zu hosten. Die derzeitigen Positionen der Aufsichtsbehörden zu Kollaborationstools werden am Beispiel von Microsoft 365 in Teil 4 Ziff. 1 dargestellt. Es handelt sich dabei um aktuelle Positionen mit oft kurzer Halbwertszeit.

Ohne Frage ist der Einsatz von Dienstleistern aus Drittstaaten derzeit rechtlich sehr heikel. Dem steht die Realität gegenüber, dass ein Großteil des Wirtschaftslebens über US-amerikanische Cloud Services abläuft, Bundes- und Landesregierungen auf sozialen Medien wie Facebook, Twitter und Instagram aktiv sind, und das 100%ige Bundesunternehmen Deutsche Bahn AG just ihre Server gegen Cloud-Dienste von Amazon und Microsoft eingetauscht hat (bit.ly/Paritaet-BahnIT).
Der Wunsch der Aufsichtsbehörden nach **eigenem Hosting und Open Source** Software ist zwar im Kern nachvollziehbar. Bei zahlreichen Unternehmen und Organisationen ist Open Source Software längst im Einsatz, doch finden sich noch nicht für alle Einsatzgebiete komfortable Lösungen. Zudem dürfte das Vorhaben, ein ei-

genes Hosting zahlreicher Systeme zu realisieren, ohne die zeitlichen und fachlichen Ressourcen dafür vorhalten zu können, oft zu einem weniger professionellen Betrieb führen als beim Cloud-Angebot. Damit steigt die Gefahr für die dort gespeicherten Daten.

Daher hat sich sogar der baden-württembergische Datenschutzbeauftragte Stefan Brink dahingehend geäußert, dass vor einer Untersagung von Kollaborationstools das **Vorhandensein zumutbarer Alternativen** zu prüfen sei (bit.ly/Paritaet-Brink).

Die Entscheidung für oder gegen ein Tool ist eine Risiko- und Gewissensentscheidung, die jeder Vorstand und jede Geschäftsführung **selbst fällen und verantworten muss**, und eine Frage der Zuversicht, ob überzogene Anforderungen und US-kritische Auffassungen der Aufsichtsbehörden durch Gerichte korrigiert werden und zugleich große Cloud-Anbieter technisch, vertraglich und lobby-seitig alles dafür tun werden, damit ihr Europageschäft nicht als illegal gilt. Und häufig wird eine solche Entscheidung nicht in einem „ganz oder gar nicht" liegen, sondern in einer risikoabhängigen Abwägung, bei der bestimmte Funktionen ungenutzt bleiben und technisch-organisatorische Maßnahmen zusätzliche Sicherheit bieten.

10. Was ist bei Open Source Software besser?

Open Source Software unterliegt selbstverständlich denselben datenschutzrechtlichen Anforderungen wie jede andere Lösung. Allerdings ist mangels aggressiv-kommerzieller Betreiber meist der „Datenhunger" zur Erfassung von Userdaten und Nutzungsverhalten zwecks Analyse, Werbung und „Upselling" ungleich geringer. Zudem besteht wegen des **frei verfügbaren Quellcodes** ein deutlich geringeres Risiko von sicherheitsrelevanten Bugs oder gar „Back Doors" für Sicherheitsdienste.
Daher sind Datenschutzbehörden bei Open Source Software in der Regel sehr wohlwollend – ganz im Gegensatz zu ihrer Einschätzung bei den großen US-Dienstleistern.

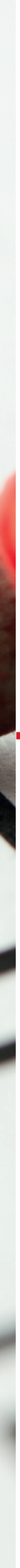
11. Gibt es neben der DSGVO noch weitere Datenschutzgesetze?

Die DSGVO soll als Europäische Verordnung alle Aspekte des allgemeinen Datenschutzrechtes EU-einheitlich abdecken; der englische Name bringt dies noch besser zum Ausdruck („General Data Protection Regulation"). Jedoch gab es einige Themen, bei denen die EU sich nicht einigen konnte und die daher von den Mitgliedsstaaten individuell geregelt werden können. Diese Regelungen finden sich in den ersten Teilen des seit 2018 geltenden **Bundesdatenschutzgesetzes (BDSG)**.
Zudem gibt es sektorenspezifisches Recht wie das Telemedienrecht (TMG) und das Telekommunikationsgesetz (TKG) deren datenschutzrechtlichen Teile ab Dezember 2021 im neuen Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) zusammengefasst sind; außerdem den Medienstaatsvertrag und einige andere Nebengesetze. Über eine neue ePrivacy-Verordnung wird in der EU seit vielen Jahren verhandelt, eine Verabschiedung ist aber nicht absehbar (bit.ly/Paritaet-ePVO).

Achtung: Im BDSG bitte nur die Normen bis einschließlich § 44 beachten – die weiteren Teile gelten für nicht von der DSGVO abgedeckte und für Sie nicht relevante Themen, wie Staatsanwaltschaften oder internationale Ehrungen.

TTDSG:
Seit Dezember 2021 gelten nicht mehr die Datenschutzregeln aus dem TMG, sondern aus dem **neuen TTDSG**. Damit wurde auch das EuGH-Urteil zu Planet49 umgesetzt. Die übrigen Regelungen wurden weitgehend unverändert aus §§ 11 ff. TMG übernommen.

Für das Datenschutzrecht und die Datenschutzaufsicht der römisch-katholischen Kirche und der Evangelischen Kirche in Deutschland gibt es statt der DSGVO eigene Datenschutzgesetze (u.a. **KDG, KDR, EKD-DSG**). Abgesehen von der Regelung von Daten über die Religionszugehörigkeit sind diese inhaltlich der DSGVO sehr ähnlich (vgl. Art. 91 DSGVO).



TEIL 3

Checkliste für den Einsatz von Kollaborationstools

Die Basics: Wer, was, wie, wo

☒ Werden **personenbezogene Daten** verarbeitet? Die Frage nach der Anwendbarkeit der DSGVO wird praktisch immer zu bejahen sein (s. Teil 2 Ziff. 2).

Es muss klar sein, wer konkret **Verantwortlicher** ist (Name z.B. des e.V. oder der gGmbH; s. Teil 2 Ziff. 1):

_____.

☐ Soll die Lösung auch **durch andere Verantwortliche** genutzt werden, d.h. durch Tochtergesellschaften, nahestehende Vereine/Verbände, Organisationen im Paritätischen (s. Teil 2 Ziff. 7)?

Wenn ja:

Wie ist das vertragliche Konstrukt dafür:

☐ Separater Vertrag mit dem Dienstleister

☐ Rahmenvertrag nebst Einzelverträgen

☐ Unternutzer des ersten Verantwortlichen (Modell „Untermieter")

☐ Sonstiges: _____.

☐ Wie ist bei Mehrfachnutzung die Trennung der Daten mehrerer Verantwortlicher abgesichert: _____.

Leistungsbeschreibung: Welches Tool zu welchem Zweck mit welchen Teilnehmern und Daten (Dokumentation und Rechenschaftspflicht, s. Teil 2 Ziff. 6)?

Name des Tools: _____.

Anbieter (vollständiger Name des Unternehmens): _____.

Allgemeine **Beschreibung des Tools** / der Nutzung (z.B. Terminsuche, Videokonferenz): _____.

Wer sind die **Betroffenen**, d.h. wessen Daten werden verarbeitet, z.B. Mitarbeiter*innen, Vereinsmitglieder (s. Teil 2 Ziff. 1 u. 4): _____.

Welche **Daten oder Arten von Daten** werden verarbeitet (z.B. Anmeldedaten incl. E-Mail-Adresse, Chatverläufe, Videokonferenz (Datum und Inhalt), ggf. Teilen des eigenen Screens): _____.

☐ Erfolgt eine Absicherung der Daten und/oder eine Einschränkung der Nutzung durch technische und organisatorische Maßnahmen (s. Teil 4 Ziff. 1. a)? Wenn ja, bitte dokumentieren (s. unten Ziff. 5).

Sind Daten von **Personen unter 16 Jahren** oder **sensible Daten** i.S.d. Art. 9 DSGVO betroffen (s. Teil 2 Ziff. 5)?

☐ Ja, Kinder (Art. 8 DSGVO)
☐ Ja, sensible Daten (Art. 9 DSGVO)
☐ Weder noch

Hosting, Betrieb und Zugriff (s. Teil 2 Ziff. 7 u. 8)

☐ ausschließlich durch den Verantwortlichen
☐ oder (auch) durch Dienstleister?
☐ Dienstleister, Subunternehmer oder Daten(zugriff) von außerhalb der EU?

☐ Werden **obige Angaben dauerhaft Bestand haben** (Dokumentation und Rechenschaftspflicht, s. Teil 2 Ziff. 6)? Wenn nein, was angesichts in Zukunft hinzukommender Features und Nutzungsmöglichkeiten typisch ist: Existiert interner Prozess, wie Änderungen erfasst und geprüft werden?

Rechtsgrundlage für die Datenverarbeitung

Vorgesehene Rechtsgrundlage(n), s. Teil 2 Ziff. 4:

☐ **Einwilligung** (meist keine gute Wahl, vgl. Teil 2 Ziff. 4)
Vorgesehener Text:

_____

_____

☐ Ist die Abgabe wirklich freiwillig?
☐ Informiertheit, Transparenz & Hinweis auf Widerspruchsrecht
Was passiert im Fall eines Widerrufs der Einwilligung? _____ .

☐ **Vertrag / Arbeitsvertrag / Betriebsvereinbarung**
☐ Besteht der Vertrag direkt mit dem Betroffenen?
☐ Ist die Datenverarbeitung beschränkt auf das aus dem Vertrag Erforderliche?

☐ **Berechtigtes Interesse**
Interessen des Verantwortlichen:

_____ .

Risiken für den Betroffenen:

_____ .

Dokumentation der Abwägung:

_____

_____ .

☐ Hinweis aufs Widerspruchsrecht.
Was passiert im Falle eines Widerspruchs? _____

Auftragsverarbeitung (AVV), s. Teil 2 Ziff. 7.

☐ AVV erforderlich?
Wenn nein: Weshalb und ggf. andere Vereinbarung (Joint Control)? _____ .

☐ AVV/SCC mit Dienstleister vereinbart
☐ Inhaltlich einschließlich der Anlagen (Art und Zwecke der Datenverarbeitung, TOMs und Subunternehmer) geprüft/ und freigegeben.

In aller Regel ja: Aufsichtsbehörden propagieren zwar eigenes Hosting von Open Source-Lösungen, aber i.d.R. nicht realistisch für Vereine, gGmbHs der Stiftungen, vgl Teil 2 Ziff. 9.

Datenübermittlung in Drittland, s. Teil 2 Ziff. 8.

☐ Staat ohne ausreichendes Schutzniveau ist involviert, z.B. USA (ausreichendes Schutzniveau u.a. in EU, EWR, Japan, Israel)

Dies ist nicht nur dann relevant, wenn der Dienstleister seinen Sitz im Drittland hat, sondern auch wenn „nur" die Server dort stehen oder dort Subunternehmer eingesetzt werden.

Wenn ja, Rechtsgrundlage für die Übermittlung bzw. den Einsatz:
☐ EU Standard Contractual Clauses (SCC)
Fassung Version: _____ .
☐ Alle Felder und Anlagen ausgefüllt
☐ Zusätzliche / ausreichende Garantien liegen vor und sind geprüft
☐ Binding Corporate Rules (welche Gesellschaften und Themen sind erfasst?)
☐ Sonstige: _____ .

Dokumentation und „Datenschutz-Bürokratie", s. Teil 2 Ziff. 6.

☐ Rechtsgrundlage(n) und ggf. Einwilligung/ berechtigtes Interesse dokumentieren
☐ Aufnahme in Verarbeitungsverzeichnis
☐ Informationspflichten (Art. 13/14 DSGVO) einschließlich Information zu Widerrufs-/Widerspruchsrecht (z.B. in Datenschutzerklärung oder Mitarbeiter-Info)
☐ Ggf. Datenschutz-Folgenabschätzung
☐ Ggf. zusätzliche technische und organisatorische Maßnahmen festlegen und dokumentieren (s. Teil 4 Ziff. 1. a)
☐ Berechtigungs-/Löschkonzept

Tools zur Online-Zusammenarbeit

www.der-paritaetische.de/tool-tipps

5:25 PM
60 %
atsApp

TEIL 4

Zwei konkrete Beispiele

Wie ist es bei Microsoft 365 und WhatsApp – und was sagen die Aufsichtsbehörden? Die Zulässigkeit und die Probleme bei Kollaborationstools sollen an zwei konkreten Anwendungen dargestellt werden.

1. Microsoft 365

a) Funktionsumfang

Microsoft 365 (früher Office 365) bündelte als Software as a Service zunächst diejenigen Dienstleistungen, für die Microsoft ursprünglich in seinen Office-Paketen Softwarelizenzen verkauft hat, also E-Mails und Kalender in Outlook nebst Word, Excel, PowerPoint etc. Dies wurde durch zahlreiche weitere Services ergänzt, darunter Sharepoint, Teams, OneDrive und einige übergreifende Mess- und Analysefunktionen (z.B. Delve). Insgesamt handelt es sich dabei inzwischen um eine kaum überschaubare (und ständig steigende) Anzahl von Programmen („Apps") und Funktionen. Zudem sind für Microsoft 365 und darin auch schon alleine für die Funktion „Teams" über den Microsoft-eigenen App Store (appsource.microsoft.com) zusätzliche Apps herunterladbar; für Microsoft 365 sind es über 3.000. Diese Nutzung zu kontrollieren, klingt zunächst nach einer kaum zu bewältigenden Aufgabe für Admins und Arbeitgeber, ist aber auch nicht grundlegend anders als die klassische Situation mit .exe-Dateien oder Browser-PlugIns. Ein erster Schritt für die juristische Analyse besteht daher darin, die gewünschten Funktionen einzugrenzen – und dies in den Konfigurationen technisch umzusetzen.

Zusätzlich zu diesen technischen Maßnahmen kann durch organisatorische Maßnahmen vorgegeben werden, welche Daten in welcher Form ausgetauscht werden dürfen. Hierzu kann z.B. gehören, dass xls-Sheets mit Gehaltsdaten nur verschlüsselt übertragen dürfen. Gemeinsam stellen solche Regeln „technische und organisatorische Maßnahmen" i.S.d. Art. 32 Abs. 1 DSGVO dar.

b) Sicht der Aufsichtsbehörden

Bewertungen der Aufsichtsbehörden betrachten vor allem die Kollaborations-App „Teams", die u.a. Chat-, Dokumenten- und Videokonferenzfunktionen verbindet und damit ein umfassendes Kollaborations-Paket anbietet. Der Zusammenschluss der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ist im Oktober 2020 in einem unveröffentlichten Entwurf einer Stellungnahme zu Microsoft 365 zu dem Ergebnis gekommen, „dass auf Basis [der Unterlagen vom Januar 2020] kein datenschutzkonformer Einsatz … möglich war." Dies klingt zunächst nach einem Todesurteil für Microsoft 365. Bei genauerem Lesen hingegen wird klar, dass die Stellungnahme überholt, unvollständig und unklar ist. Unter anderem wurden veraltete Vertragsbedingungen von Microsoft (die „Online Services Terms", OST) zu Grunde gelegt und das so wichtige EuGH-Urteil Schrems II (siehe Teil 2 Ziff. 8) nicht berücksichtigt. Selbst der stets sehr auf Datenschutz bedachte heise-Verlag brandmarkte den Entwurf – der nur durch eine Anfrage über Frag Den Staat öffentlich wurde – als „irgendwo zwischen unverschämt und weltfremd" (bit.ly/Paritaet-heise). Auch die „Orientierungshilfe Videokonferenzsysteme" der DSK vom Oktober 2020 ist weder für die Video-Funktionen von Microsoft 365 (Teams, Skype, Skype for Business) noch für Zoom oder andere Produkte hilfreich. Neben den – zumindest für kleinere Organisationen – praxisfernen Vorschlägen, Videokonferenzsysteme selbst zu betreiben, besteht sie weitgehend aus allgemeinen rechtlichen und technischen Ausführungen. Die Berliner Datenschutzbeauftragte bezeichnet den Einsatz von Microsoft 365 in Pressemitteilungen sogar als unzulässig.

Diese Darstellung zeigt aber nur eine Seite der Datenschutzbehörden. Denn zugleich begleitet die Aufsichtsbehörde in Baden-Württemberg die dortige Kultusministerin bei der Nutzung von Microsoft 365 an Schulen – die dafür prompt von Datenschützern einen Big Brother Award verliehen bekam (bit.ly/Paritaet-BW, bit.ly/Paritaet-BB). und auch weitere Aufsichtsbehörden verhalten sich konstruktiv im Umgang mit Microsoft. Microsoft seinerseits hat mit dem neuen Vertrags-Setup (Product & Service Terms plus Data Privacy Addendum) intern bereits die neuen SCC umgesetzt (bit.ly/Paritaet-MSneu).

c) Lösungen in der Praxis

Zwischen technischer Innovation, zusätzlicher Datennutzung, rechtlichen Änderungen, überhöhten Anforderungen der Aufsichtsbehörde und Anpassungen seitens der Anbieter wird es immer Diskrepanzen und bisweilen ein Katz-und-Maus-Spiel geben.

Zugleich stehen Organisationen unter dem Zwang, Anforderungen der Digitalisierung umzusetzen – und dabei möglichst nicht der Letzte zu sein. Zu Recht äußerte die schon erwähnte Aufsichtsbehörde aus Baden-Württemberg sehr praxisnah, dass pauschale Aussagen zur Zulässigkeit bestimmter Softwareprodukte wie z.B. Microsoft 365 unangemessen seien und zudem das Vorhandensein zumutbarer Alternativangebote zu berücksichtigen sei. (bit.ly/Paritaet-Brink). Gleichwohl setzen viele öffentliche Stellen Microsoft 365 ein, und die Deutsche Bahn als bundeseigenes Unternehmen verkündete jüngst, ihre gesamten Rechenzentren in die Clouds von Microsoft und Amazon zu verlegen (bit.ly/Paritaet-DB). Der französische Conseil d'État hat eine Klage abgewiesen, mit der einer staatlichen Gesundheitsplattform untersagt werden sollte, sensible Daten in europäischen Rechenzentren der Microsoft-Cloud Azure zu speichern (bit.ly/Paritaet-FR). In beiden Fällen wurden die Daten u.a. durch Verschlüsselung und Standortvorgaben besonders geschützt.

Es ist nicht nachvollziehbar, wenn der Staat diese Angebote einerseits selbst nutzt, sie aber andererseits gegenüber gemeinnützigen Organisationen als datenschutzwidrig untersagt. Wie bei der Bahn sollte in dieser unklaren Rechtslage überlegt und dokumentiert sein, wie überflüssige und bedenkliche Funktionen deaktiviert und Risiken reduziert werden, und welche Nachteile bei Alternativen bestehen würden (wie: von dem Tool abzusehen, selbst hosten, einen anderen Anbieter wählen). Dabei ist es Aufgabe von Vorstand bzw. Geschäftsführung und nicht des*der Datenschutzbeauftragten, die Restrisiken zu verstehen und zu akzeptieren, oder sich für Alternativen zu entscheiden.

2. WhatsApp und andere Apps, die das gesamte Adressbuch hochladen und synchronisieren (Instagram, Snapchat)

WhatsApp ist extrem praktisch – fast jede*r in Deutschland hat es, fast jede*r ist erreichbar, sei es per Chat, Anruf oder Video, direkt oder in Gruppen. Dass so viele Bekannte sofort auffindbar sind, liegt daran, dass WhatsApp und einige andere Apps sich vom Smartphone den Zugriff auf das volle Adressbuch einräumen lassen. Dies wird beim ersten Start auf die Server von WhatsApp hochgeladen und in der Folge weiter synchronisiert. So landen die Daten der im Adressbuch gespeicherten Personen auf US-Servern von WhatsApp und ggf. auch bei der Muttergesellschaft Facebook, ohne dass die Betroffenen informiert wurden oder gar zugestimmt haben.
Schon aus diesem Grund wird der betriebliche Einsatz von WhatsApp unisono als unzulässig angesehen – die Fragen zum Transfer in Drittländer müssen da gar nicht weiter beleuchtet werden (bit.ly/Paritaet-WhatsApp).
Zulässige Ausnahmen sind möglich, wenn das Hochladen verhindert oder stark eingeschränkt wird, indem ein separates WhatsApp-Telefonbuch verwendet wird, oder wenn die Verwendung und das Adressbuch tatsächlich auf den rein persönlich-familiären Bereich beschränkt wird. Denn im letztgenannten Fall ist die DSGVO nicht anwendbar (Teil 2 Ziff. 2). Dann muss das Adressbuch aber auch wirklich entsprechend beschränkt sein – Kollegen oder gar die Daten der Pflegebedürftigen von mobilen Pflegediensten dürfen dann nicht abgespeichert werden.

Dies zeigt das Datenschutz-Dilemma bei sozialen Medien und unter dem Netzwerkeffekt der Kommunikationsmittel: Zwar kann man in seiner Organisation „nach unten" anweisen, dass WhatsApp & Co. nicht verwendet werden dürfen. Wenn aber ein wichtiger externer Ansprechpartner, auf dessen Erreichbarkeit man angewiesen ist, vielleicht ein*e Politiker*in oder Entscheider*in, am besten per WhatsApp erreichbar ist, unterliegen Mitarbeiter*innen oft dem faktischen Zwang, sich auf dessen Kommunikationsmittel einzulassen.

Besondere Vorsicht ist beim Einsatz von WhatsApp & Co. im Krankenhaus- und Pflegedienst oder bei sonstigen sensiblen Daten geboten (siehe Teil 2, Ziff. 5). Die DSK hat auch hierzu strenge Anforderungen aufgestellt (bit.ly/Paritaet-DSKmessenger). Alternativen in dieser Branche sind spezielle und gesicherte Apps wie Myo.

TEIL 5

Dos und Don'ts und häufig gestellte Fragen

Dos

Nachdenken: Was machen Sie, wie wichtig ist das und was könnte realistisch (nicht im theoretischen Worst Case) passieren? Falls morgen in der Bild-Zeitung steht, was Sie getan haben: Wäre das eine gute oder eine schlechte Mitteilung? Wäre es schlimmer, nicht zu digitalisieren, oder für eine wichtige Aufgabe vor einer unklaren Rechtslage ein Risiko einzugehen?

Daumenregel: Wenn die Beteiligten wissen, was mit ihren Daten passiert und freiwillig dabei sind, ist es eher unkritisch, selbst wenn manche Datenschutz-Formalitäten nicht ganz streng eingehalten werden. Beispiel: Freiwillige Teilnahme an Videokonferenz. Wenn die Beteiligten oder gar Unbeteiligte nicht wissen, was mit ihren Daten passiert, ist es eher bedenklich und kann außerdem schnell dazu führen, dass Betroffene sich beschweren. Beispiele: Heimliche Analyse der Teilnahme und Aktivität von Usern; Daten von Unbeteiligten sammeln.

Suchmaschine nutzen: Im Zweifel erst mal selbst nachschlagen – meistens ist man nicht der*die Erste, der*die sich diese Frage stellt.

Fragen: Wenden Sie sich an Ihre*n Vorgesetzte*n, wenn vorhanden die Rechtsabteilung oder den eigenen Datenschutzbeauftragten.

Don'ts

Blind den Angaben der Dienstleister vertrauen: Natürlich sagt jeder Dienstleister, dass seine Lösung völlig datenschutzkonform sei. Er will sie ja verkaufen.

Etwas tun, was Sie im realen Leben auch nicht dürfen: Im Konferenzraum würden Sie auch nicht heimlich Fotos Ihrer Kollegen machen – wieso sollte es bei Zoom gehen?

„Ganz oder gar nicht"-Denkweise: Jemand hat „Bedenken" bei einem Tool? Haken Sie nach, um zu verstehen, wo das Problem konkret liegt. Vielleicht kann die kritisierte Funktion einfach deaktiviert werden, oder Sie setzen technisch-organisatorische Mittel ein, um das Risiko zu reduzieren. Dies beginnt damit, Daten zu verschlüsseln und Kommunikationskanäle gezielt auszuwählen. Das ist besser als das Tool ganz ungesichert oder gar nicht zu nutzen.

Lästern: Noch dümmer als in E-Mails – Sie wissen nie, wer das alles liest/hört/ansieht.

IT-Sicherheit aus den Augen verlieren: Denken Sie nicht nur an juristische Risiken. Wie sicher ist Ihr Passwort, wer hat Einblick in Ihren Kalender und kann sich in Videokonferenzen einwählen oder auf gesharte Dokumente zugreifen? Wissen Sie noch, wem Sie letztes Jahr Zugriffsrechte auf vertrauliche Dokumente gegeben haben?

Nur Bedenken und Risiken sehen: Bei allem gibt es Bedenken, aber auf Digitalisierung zu verzichten ist keine Lösung. Kann ein wirkliches Risiko bestehen (wie bei Gesundheitsdaten oder anderen sensiblen Daten) oder ist es nur ein theoretisches Problem?

Gibt es in der DSGVO Ausnahmen für eingetragene Vereine und sehr kleine Organisationen, die sich keinen Datenschutz leisten können?

Die DSGVO gilt gleichermaßen für sämtliche „Verantwortlichen" (s. Teil 2 Ziff. 1), unabhängig von der Rechtsform. Allgemeine Anforderungen wie das Erfordernis einer Rechtsgrundlage für die Datenverarbeitung, Informationspflichten, Betroffenenrechte etc. gelten wie für alle anderen Verantwortlichen. In Erwägungsgrund 13 der DSGVO werden Kleinstunternehmen sowie kleine und mittlere Unternehmen gewürdigt, aber nicht prinzipiell bessergestellt. Allerdings gibt es, gerade bei der Frage nach dem angemessenen Aufwand für die eigene IT-Sicherheit, zahlreiche Abwägungsmöglichkeiten in der DSGVO. Hier können kleine Organisationen argumentieren, dass bei ihnen der gleiche Aufwand wie bei einem Konzern nicht angemessen sei.

Ein schwacher Trost: Die Bußgelder bemessen sich nach dem Umsatz und ein wenig auch nach der wirtschaftlichen Zumutbarkeit. Insofern drohen dort geringere Summen als bei einem umsatzstarken Betrieb.

Die DSGVO verwendet den Begriff „Unternehmen" übrigens im Sinne des EU-Rechts, wo es auch nichtkommerzielle Organisationen einschließt und nicht – wie im Deutschen – nur „Firmen" meint.

Bringt die Gemeinnützigkeit DSGVO-Erleichterungen mit sich?

Nein. Steuerliche Aspekte spielen für die DSGVO keine Rolle. Zu kleinen und mittleren Unternehmen siehe oben.
Unter Umständen kann bei der Bewertung eines „Berechtigten Interesses" (Teil 2 Ziff. 4) positiv berücksichtigt werden, dass es sich um gemeinnützige Ziele der Organisation handelt.

Gibt es Ausnahmen für die Presse-/Medienarbeit?

Nach Art. 85 DSGVO sollen die Mitgliedsstaaten für Tätigkeiten, die der Meinungs- und Informationsfreiheit dienen, Ausnahmen von einigen Teilen des DSGVO vorsehen. Damit wird das im deutschen Grundgesetz und der EU-Grundrechtecharta vorgesehene Recht auf Presse- bzw. Meinungsfreiheit umgesetzt (Art. 5 GG, Art. 11 EU-GRCh). In Deutschland ist dies durch den Medienstaatsvertrag und die Landespressegesetze erfolgt. Für journalistische Zwecke gelten die meisten Teile der DSGVO daher nicht. Dafür müssen diese journalistischen Daten (wie z.B. Rechercheergebnisse, Informationen über Informant*innen) ihrerseits von den anderen Daten getrennt werden.

Gilt die DSGVO auch für private Tätigkeiten?

Bei rein persönlichen oder familiären Tätigkeiten ist die DSGVO nicht anwendbar. Diese Ausnahme wird von den Gerichten sehr eng ausgelegt. Schon Aufnahmen des Bürgersteigs durch eine private Überwachungskamera oder Aufnahmen einer „Dash-Cam" aus dem Privatwagen fallen meist nicht mehr unter diese Ausnahme, sondern unterliegen der DSGVO (s. Teil 2 Ziff. 2).

Kann ich als Arbeitgeber von meinen Mitarbeiter*innen verlangen, eine notwendige Einwilligung zu unterschreiben? / Kann mein Arbeitgeber mich zwingen, eine Einwilligung abzugeben?

Nein. Einwilligungen müssen freiwillig erklärt werden, und außerdem sind sie jederzeit frei widerrufbar. Daher sind sie kein guter Weg, um im Betrieb eine Rechtsgrundlage für eine Datenverarbeitung zu schaffen (s. Teil 2 Ziff. 4). Das Berechtigte Interesse, ein (Arbeits-)Vertrag oder eine Betriebsvereinbarung ist meist die passendere Rechtsgrundlage.

Darf ich die Aufnahmefunktion in der Videokonferenzsoftware nutzen, um das Gespräch mit meinen Kollegen festzuhalten?

Nein – das würde man ja im wahren Leben auch nicht machen.

Eine Ausnahme kann z.B. gemacht werden, wenn es sich bei dem Videotermin um eine Schulung handelt, die für weitere interessierte Mitarbeiter*innen aufgenommen werden soll, und der*die Referent*in sowie alle, die z.B. durch Video oder Namenseinblendung erkennbar sind, ausdrücklich einverstanden sind.

Weitere Ausnahmen sind denkbar, um in einer virtuellen Vorstands- oder Mitgliederversammlung bei Einverständnis aller Teilnehmenden den ersten Teil der Sitzung aufzunehmen, in dem die „anwesenden" Teilnehmenden per Video identifiziert werden und damit die Beschlussfähigkeit festgestellt wird. Anders als bei dem vorher genannten Schulungsvideo ist hierbei aber erforderlich, dass der Zugriff und die Speicherdauer der Aufnahme restriktiv festgelegt werden (z.B. Zugriff nur durch Vorsitzenden und Stellvertreter im Vier-Augen-Prinzip und nur im Fall von begründeten Zweifeln an der Beschlussfähigkeit; Löschung nach Ablauf von Anfechtungsfristen).

Darf ich Screenshots von der Videokonferenz machen und diese posten?

In normalen Videokonferenzen: Nein. Sofern der Screenshot nur eine öffentliche Präsentation und keinen Teilnehmenden zeigt, dürfte dies wie bei echten Konferenzen akzeptabel sein. Im Übrigen ist es nicht zulässig, zumal die Aufgenommen – anders als bei einem Selfie oder einem Fotografen bei einem echten Event – nicht damit rechnen, aufgenommen zu werden und daher der Aufnahme nicht widersprechen können. Weitere Ausnahmen sind denkbar, wenn die Teilnehmende wirklich einverstanden sind oder prominente Redner*innen bei großen, öffentlichen Veranstaltungen sprechen. Letztlich dürfte die Akzeptanz der Abgebildeten nicht anders sein als bei klassischen Veranstaltungen: Der*die eine steht gerne im Rampenlicht und freut sich darüber, ein*e andere*r nicht.

Bitte passen Sie bei solchen Screenshots auch auf, welche Informationen Sie damit teilen. Die Verteidigungsministerin eines EU-Staates veröffentlichte während einer vertraulichen Sitzung der Verteidigungsminister auf Twitter stolz einen Screenshot, auf dem sie und die anderen Teilnehmer zu sehen waren. Was sie nicht bedachte: Auf dem Screenshot waren weitere Angaben zu sehen, aus denen man auf die Einwahldaten schließen konnte. Ein Journalist erkannte dies und wählte sich zur Verwunderung der zahlreichen Minister live ein.

Wie kann ich verhindern, dass sich fremde Personen einwählen?

Egal ob Unbekannte sich einwählen, um laut zu stören oder um heimlich mitzuhören: Dies kam zu Beginn der Corona-Zeit durchaus vor und gilt es unbedingt zu vermeiden. Zugangsbeschränkungen können dadurch erfolgen, dass für die Einwahl zusätzlich ein Passwort erforderlich ist, und/oder durch die Option, dass jeder Teilnehmende aktiv „eingelassen" werden muss. Bei rein internen Konferenzen können auch sog. Gastzugänge deaktiviert werden.

Darf ich Teilnahme und Beteiligung dokumentieren und auswerten?

Hier gilt im Wesentlichen das Gleiche wie bei Präsenzterminen: Außer in üblichen Teilnahmeprotokollen sollte dies nur mit einem rechtlich relevanten Grund erfolgen, z.B. wenn die Teilnahme an einer Pflichtschulung zum Arbeitsschutz dokumentiert werden soll. Zudem sind Verhaltens- und Leistungskontrollen zu vermeiden bzw. arbeitsrechtlich die Rechte des Betriebsrates zu beachten.

Was ist mit fremden Personen im Hintergrund?

Jede*r kennt das: Während einer langen Videokonferenz kommt ein Kind oder eine andere Person in den Kameraausschnitt. Die Aufsichtsbehörden legen viel Wert darauf, dass dies verhindert werden muss bzw. nur mit Zustimmung erfolgt. Dies kann z.B. durch die Funktion erfolgen, mit der der Hintergrund verschwommen dargestellt wird. Vielleicht sollten Arbeitgeber, Mitarbeiter*innen und Aufsichtsbehörden auch einfach etwas entspannter sein – auch früher hat manch eine*r bei Schulschließungen Kinder mit ins Büro genommen, die dann von den Kollegen gesehen werden konnten.

Was ist mit privaten / nebensächlichen Äußerungen z.B. im Chat oder in Videokonferenzen?

Bei Videokonferenzen ist es hilfreich, wenn – wie in echten Meetings – nicht nur über die Fachthemen gesprochen wird (https://www.der-paritaetische.de/themen/bereichsuebergreifende-themen/gleichimnetz/webzeugkoffer/). Damit geht einher, dass dort auch private und vielleicht sensible Informationen mitgeteilt werden – der letzte Urlaub, wie sich der Sohn einen Arm gebrochen hat, dass man heute Morgen erst noch den pflegebedürftigen Vater versorgen musste. So werden Daten mitgeteilt, die privat und manchmal auch besonders sensibel sind und nach Art. 9 DSGVO besonders geschützt werden. Dieser private Teil sollte gehandhabt werden wie nach einem echten Treffen: Wer in größerer Runde ohne Not Privates äußert, kann von den Teilnehmer*innen nicht strengste Geheimhaltung erwarten. Es sollte aber mit einem angemessenen Maß an Respekt und Vertraulichkeit behandelt werden.

Unser Kollaborationstool wurde vor einem Jahr vom Datenschutz zur Nutzung freigegeben. Jetzt gibt es neue Features und die Möglichkeit, Erweiterungen herunterzuladen. Das ist von der Freigabe mit umfasst, oder?

Nein – Software as a Service entwickelt sich ständig weiter, und bei der Nutzung über den Browser müssen User kein Update installieren. Dies bedeutet aber nicht, dass bei der seinerzeitigen Freigabe Hellseher am Werk waren. Die Organisation sollte, abhängig von Risiko und Relevanz des Tools, regelmäßig überprüfen, ob es alle Funktionen des Tools im Blick hat und ob IT-Sicherheit, Dokumentation, Rechtsgrundlagen und ggf. AVV, Datenschutz-Folgenabschätzung sowie Data Transfer Assessment noch die Realität abbilden.

Wie kann ich die Nutzung einschränken und dadurch sicherer machen?

Dies kann nach Art. 32 DSGVO durch technische und/oder organisatorische Maßnahmen erfolgen. Technik und Organisation können auch ineinandergreifen, z.B. durch die Anweisung zur Nutzung bestimmter Technologien. Dies muss nicht unbedingt Hightech sein – auch die Anweisung, Gehaltsdaten nur in verschlüsselten xls-Dateien zu versenden, kann eine geeignete technisch-organisatorische Maßnahme darstellen (vgl. Teil 4 Ziff. 1 a).

Darf ich auf meinem privaten Smartphone oder Notebook das Kollaborationstool herunterladen, mich einloggen und Dateien herunterladen?

Die Nutzung von Privatgeräten und „Bring Your Own Device" sind weit verbreitet und nicht grundsätzlich verboten. Allerdings muss der Arbeitgeber als Verantwortlicher dann sicherstellen, dass er seine datenschutzrechtlichen Pflichten wie IT-Sicherheit, Lösch- und Berechtigungskonzepte sowie z.B. Auskunftsersuchen von Dritten auch bezüglich der Daten auf dem Privatgerät erfüllen kann – auch wenn der*die Mitarbeiter*in die Organisation verlassen hat. Dies gelingt kaum einem Verantwortlichen, weshalb dienstliche Smartphones datenschutzrechtlich die deutlich bessere Wahl sind.

Können wir die Mitgliederversammlung unseres Vereins per Videokonferenz durchführen?

Dies ist keine datenschutzrechtliche Frage, sondern eine Frage des Vereins- und aktuell des „Corona-Rechts" (siehe Rechts-Fachinfo des Paritätischen Gesamtverbands unter www.der-paritaetische.de/digitale-mv).

Wieso wird es bei WhatsApp & Co. so kompliziert gemacht? SMS verschicke ich doch auch, ohne Datenschutzverträge abzuschließen.

Bei der Risikobewertung von elektronischen Kommunikationsmitteln – von der E-Mail bis Zoom – wird zu Recht oft der Vergleich gezogen, dass auch bei Telefon, Fax & Co. vertraulichste Informationen übertragen wurden, ohne mit dem Diensteanbieter komplizierte Datenschutzverträge vereinbaren zu müssen. Und seit Snowden ist bekannt, dass das Telefonnetz von US-Geheimdiensten ähnlich überwacht wurde wie E-Mails.

Dienste, die das Telekommunikationsnetz nicht wie z.B. Telefon und Telefax unmittelbar nutzen, sondern ihren Dienst in digitale Daten verarbeiten und „oberhalb" des Netzes übermitteln, werden „Over The Top"-Dienste genannt (OTT). Der EuGH hat 2019 am Fall von Googles Gmail-Dienst entschieden, dass Gmail als OTT kein Telekommunikationsdienst ist. Dies hat zweierlei zur Folge: Bei OTT-Diensten wie Gmail oder Skype muss man über den Datenschutz hinaus nicht noch zusätzliche telekommunikationsrechtliche Pflichten beachten. Umgekehrt kann man den datenschutzrechtlichen Anforderungen aber auch nicht entgehen, indem man es mit einem echten Telekommunikationsdienst gleichsetzt.

Allerdings kann bei einer Risikobewertung durchaus herangezogen werden, dass auch bei einem Verzicht auf das Kollaborationstool und der folgenden Nutzung des klassischen Telefonnetzes die Überwachungsrisiken keineswegs eliminiert wären. Hinweis: Im Rahmen der Novellierung des Telekommunikationsgesetzes zur Umsetzung der EU-Richtline 2018/1972 („Kodex für die elektronische Kommunikation") kann sich diese Rechtslage kurzfristig ändern.

Ist Open Source datenschutzrechtlich besser?

Open Source Software unterliegt datenschutzrechtlich den gleichen Anforderungen wie jede andere Software. Allerdings werden im Betrieb meistens weniger Daten gesammelt, und Open Source Software gilt als sicherer und transparenter (s. Teil 2 Ziff. 10). Daher sind Datenschutzbehörden bei Open Source Software in der Regel recht wohlwollend.

Wie viele Datenschutzbehörden gibt es in Deutschland?

In Bayern gibt es zwei Datenschutz-Aufsichtsbehörden: Eine für den behördlich-öffentlichen Sektor, und eine für den privat-zivilen Bereich einschließlich gemeinnütziger Organisationen. Mit den Aufsichtsbehörden der anderen 15 Bundesländer sowie dem Bundesbeauftragten gibt es 18 Datenschutzbeauftragte, die sich in der „Datenschutzkonferenz" des Bundes und der Länder informell abstimmen, kurz DSK. Die DSK ist jedoch kein offizielles Gremium und keine eigene Aufsichtsbehörde.
Zusätzlich gibt es in Deutschland noch Aufsichtsbehörden für den Kirchendatenschutz (siehe Teil 2 Ziff. 11) sowie Datenschutzaufsicht durch die Landesmedienanstalten.

Heißt es DSGVO oder DS-GVO?

Der offizielle Kurztitel der Verordnung (EU) 2016/679 lautet in der deutschen Fassung „Datenschutz-Grundverordnung". Daher übernehmen viele den Bindestrich auch in die Abkürzung, insbesondere die Aufsichtsbehörden und einige Verlage („DS-GVO"). Viele andere – und auch der Bundesgerichtshof – kürzen es ohne Bindestrich ab („DSGVO"). Da es keine offizielle Abkürzung gibt, ist keines von beidem falsch, und bei beiden Varianten ist klar, was gemeint ist.

TEIL 6

Anhang

Liste der Tool-Links aus den Tool-Tipps

Vollständige Präsentation im Webzeugkoffer vom Projekt #GleichImNetz unter
www.der-paritaetische.de/tool-tipps

	Thema	Tools
1	**Termin finden**	https://www.nuudel.de
		https://www.der-paritaetische.de/themen/bereichsuebergreifende-themen/gleichimnetz/webzeugkoffer/faq/doodle-dudle-foodle-co-was-ist-das-beste-tool-zur-terminfindung/
2	**Terminübersicht schaffen**	Google Calender / Apple Calender / Outlook
		GMX, Web.de, Posteo
		Teamarbeits-Suiten
		Kalender in der Nextcloud
		http://www.teamup.com
3	**Sich im Team besprechen**	
3.1	**Chatten**	https://wire.com/de/
		Slack, MS Teams
		https://www.der-paritaetische.de/themen/bereichsuebergreifende-themen/gleichimnetz/webzeugkoffer/faq/whatsapp-und-all-die-anderen-messenger/
3.2	**Telefonkonferenzen**	http://www.meebl.de
		https://www.phonesty.de
		https://www.freetelco.de
		https://www.teltarif.de/i/konferenz.html?page=all
		https://www.der-paritaetische.de/themen/bereichsuebergreifende-themen/gleichimnetz/webzeugkoffer/faq/wie-plane-ich-eine-telefonkonferenz/
3.3	**Videokonferenzen**	https://www.der-paritaetische.de/themen/bereichsuebergreifende-themen/gleichimnetz/webzeugkoffer/faq/wie-organisiere-ich-eine-videokonferenz/
		https://jitsi.rocks/
3.4	**Entscheidungen treffen/ Argumente austauschen**	https://www.tricider.com/
		https://jugend.beteiligen.jetzt/werkzeuge/entscheidungshilfe
4	**Aufgaben verteilen**	Google Tasks, Microsoft To-Do
		https://tasks.org/
		Trello, Asana; Meistertask, Factro; Wekan
		https://www.capterra.com.de/directory/10030/task-management/software?sort=reviews
5	**Texte bearbeiten**	
5.1	**Notizen machen**	https://pad.systemli.org
		https://pad.foebud.org/
		https://www.der-paritaetische.de/themen/bereichsuebergreifende-themen/gleichimnetz/webzeugkoffer/faq/etherpad-und-datenschutz-was-muss-ich-dazu-wissen/

5.2	**Dokumente erstellen**	Collabora als App unter Nextcloud
		Google Docs
6	**Dateien weitergeben**	Eigene Cloud (Nextcloud, Owncloud)
		https://wetransfer.com/
		https://send.firefox.com/
		https://mega.nz/
		https://www.heise.de/tipps-tricks/WeTransfer-Diese-Alternativen-gibt-es-4435985.html
7	**Präsentieren**	
7.1	**Präsentation erstellen**	https://prezi.com/
7.2	**Whiteboards erstellen**	https://www.webwhiteboard.com/
		https://awwapp.com/
		https://witeboard.com/
		https://de.padlet.com/
		https://www.miro.com
7.3	**Wortwolken erstellen**	http://www.Wortwolken.com
7.4	**Live-Umfragen machen**	https://pingo.coactum.de/
		https://www.mentimeter.com/
		https://tedme.com/
8	**Öffentlichkeitsarbeit**	
8.1	**Social Media Manager**	https://tweetdeck.twitter.com/
		https://www.facebook.com/creatorstudio
		Redaktionsplan Braunschweigische Stiftung: https://t1p.de/3zz3
8.2	**Infografiken, Facepics**	https://www.canva.com
		https://www.der-paritaetische.de/themen/bereichsuebergreifende-themen/gleichimnetz/webzeugkoffer/faq/kostenlose-fotos-aus-dem-netz/
8.3	**Online Stories**	https://wakelet.com/
9	**Diverses**	
9.1	**Links sammeln**	https://www.diigo.com
		https://www.bibsonomy.org/?lang=de
9.2	**Umfragen machen**	https://www.surveymonkey.de/
		https://crowdsignal.com/
		https://www.limesurvey.org/de/
		https://www.google.de/intl/de/forms/about/
9.3	**Zu Veranstaltungen einladen**	https://eveeno.com/de/
		https://www.eventbrite.de/
10	**Neue Tools finden und ausprobieren**	https://www.capterra.com.de/
		https://trusted.de/
		https://www.getapp.de/
		https://projectprivacy.eu/de/

WEBZEUGKOFFER

alles drin, was du brauchst!

Die Online-Welt bietet unglaublich viele Möglichkeiten, unsere Öffentlichkeits- oder auch Zusammenarbeit einfacher, schöner und spielerischer zu gestalten. Und das orts- und zeitunabhängig.
In unserem prall gefüllten Webzeugkoffer finden sich Anleitungen, Empfehlungen und Tipps zu Social Media-Kanälen und diversen Werkzeugen zur digitalen Kommunikation und Zusammenarbeit.
Einfach mal durchstöbern und inspirieren lassen!

www.der-paritaetische.de/webzeugkoffer

DER PARITÄTISCHE GESAMTVERBAND

#gleich im NETZ

Impressum

Herausgeber

Der Paritätische Gesamtverband
Oranienburger Str. 13-14
10178 Berlin
Tel. 030 24636-0
Fax. 030 24636-110
Homepage: www.paritaet.org

Verantwortlich im Sinne des Presserechts

Dr. Ulrich Schneider

Autor

Dr. Olaf Koglin, olaf@koglin.de, www.linkedin.com/in/OlafKoglin, Twitter: @_CookieBar

Redaktion

Werner Hesse, Der Paritätische Gesamtverband
Kay Schulze, Der Paritätische Gesamtverband

Fotos

Titelbild: von kras99 / Adobe Stock, Bild Seite 4 von VisualGeneration / Adobe Stock, Bild Seite 8 von WrightStudio / Adobe Stock, Bild Seite 20 von Kenishirotie / Adobe Stock, Bild Seite 26 von tashatuvango / Adobe Stock, Bild Seite 30 von sosiukin / Adobe Stock, Bild Seite 38 von Mrak / Adobe Stock, Checklisten-Form: rawpixel.com / Post-It-Zettel: rawpixel.com / Freepik, Bild Rückseite Dayne Topkin / Unsplash

Gestaltung

Lena Plaut, Der Paritätische Gesamtverband

Berlin, 1. Auflage November 2021

CC-BY-SA

Gefördert vom:

Bundesministerium
für Familie, Senioren, Frauen
und Jugend

DER PARITÄTISCHE

Wer sich mit seinem Engagement sehen lassen kann, braucht sich auch im Netz nicht zu verstecken.

Jetzt Mitglied auf www.wir-sind-paritaet.de werden.

WIR SIND PARITÄT
www.wir-sind-paritaet.de