RDSK

Datenschutzrechtliche Eckpunkte zum Einsatz von Kollaborationssystemen

Stand: Februar 2021

I. Ausgangslage

Spätestens seit dem Inkrafttreten der coronabedingten Abstandsregelungen ist der Einsatz elektronischer Plattformen, die die ortsunabhängige Kommunikation und Zusammenarbeit zwischen mehreren Beteiligten ermöglichen (im Folgenden: Kollaborationssysteme) in den Fokus gerückt. Sie ermöglichen u. a. die folgenden Funktionen: Mailversand, Telefon- und Videokonferenz, Teamräume, Chats sowie gemeinsame Bearbeitung von Dokumenten. Besonders hoch ist die Nachfrage nach Videokonferenzen für Besprechungen, virtuelle Versammlungen, Bewerbungsgespräche, Publikumsbefragungen und vieles mehr. Angesichts der erheblichen Vorteile der virtuellen Kommunikation und Zusammenarbeit ist damit zu rechnen, dass die Kollaborationssysteme dauerhaft wichtige Werkzeuge für die Zusammenarbeit im öffentlich-rechtlichen Rundfunk und mit Externen bleiben werden.

Der Einsatz derartiger Plattformen muss allerdings datenschutzkonform sein. Denn bei ihrer Nutzung werden insbesondere folgende personenbezogene Daten verarbeitet:

- Namen und Kontaktdaten der User*innen
- Inhalte der Videokonferenz, also Ton und (Bewegt-)Bild, des Chats, der Dateien (Dokumente); dazu können auch besonders sensible Daten im Sinne von Art. 9 DSGVO gehören (z. B. körperliche Eigenschaften, politische Einstellungen etc.).
- Metadaten (z.B. zum konkreten Standort oder verwendeten Rechner)

II. Anforderungen in datenschutzrechtlicher Hinsicht

1. Schutzbedarfsfeststellung

Vor einer Auswahlentscheidung für ein Kollaborationssystem muss der Verantwortliche (im Folgenden: die Rundfunkanstalt) das angemessene Schutzniveau für die personenbezogenen Daten festlegen, die mittels der Plattform – voraussichtlich – verarbeitet werden. Die an das System zu stellenden Anforderungen in datenschutzrechtlicher Hinsicht richten sich nach dem Schutzbedarf der Daten, den die Rundfunkanstalt auf dieser Grundlage festgestellt hat. Ausschlaggebend ist die am höchsten ermittelte Schutzklasse der einzelnen Datenkategorien. Gegebenenfalls muss die Rundfunkanstalt durch geeignete technische und/oder organisatorische Maßnahmen verhindern, dass eine Kollaborationsplattform für Zwecke bzw. Anlässe genutzt wird, bei denen nicht hinreichend gewährleistet ist, dass personenbezogene Daten verarbeitet werden, die einer höheren Schutzklasse als der zugelassenen unterliegen (siehe auch III.).

2. Datenschutzrechtliche Anforderungen

Die Kollaborationsplattform muss alle zwingenden datenschutzrechtlichen Anforderungen, insbesondere die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO, u. a. Transparenz, Zweckbindung und Datensparsamkeit) sowie für die Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO) erfüllen. Die Möglichkeit datenschutzfreundlicher Voreinstellungen (Art. 25 DSGVO) muss gegeben sein. Unter den in Art. 35 DSGVO genannten Voraussetzungen muss die Rundfunkanstalt dazu gegebenenfalls eine Datenschutzfolgenabschätzung durchführen. Eine solche ist jedenfalls erforderlich, wenn das betreffende System den Einsatz neuer Technologien wie Sprach-, Gesichts- oder Stimmerkennung oder die Transkription ermöglicht bzw. vorsieht.

3. Betriebsmodelle

Grundsätzlich kann die Rundfunkanstalt wählen, ob sie eine Kollaborationsplattform selbst oder gemeinsam mit anderen Rundfunkanstalten oder Einrichtungen betreibt, oder aber den Online-Dienst eines externen Anbieters nutzt. Sofern sie sich für einen externen Dienstleister entscheidet, muss sie allerdings Folgendes beachten:

Je nachdem, um welches Fremdsystem es sich handelt, werden bei dessen Nutzung personenbezogene Daten ganz oder teilweise auf Server in Nicht-EU-Staaten, insbesondere in die USA übermittelt. Der EuGH hat mit Urteil vom 16. Juli 2020 („Schrems II“) die Privacy Shield-Vereinbarung für unwirksam erklärt und hält zudem auch die von der EU-Kommission bislang entwickelten Standardvertragsklauseln ohne zusätzliche Garantien und Maßnahmen für keine hinreichende Rechtsgrundlage für den Datentransfer in die USA. Empfehlungen zu dahingehenden technischen und vertraglichen Maßnahmen hat der Europäische Datenschutzausschuss (EDSA) am 10. November 2020 veröffentlicht (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf).

Daraus folgt, dass Systeme von US-Anbietern wie Microsoft, Zoom oder anderen nur dann DSGVO-konform genutzt werden können, wenn die Rundfunkanstalt neben der Vereinbarung der Standardvertragsklauseln zusätzliche Garantien und Maßnahmen durchsetzt, die ein der DSGVO entsprechendes Datenschutzniveau gewährleisten.

Eine Einschränkung gilt für die Verarbeitung von streng vertraulichen personenbezogenen Daten:

Soll eine Kollaborationsplattform (auch) eingesetzt werden können, um streng vertrauliche personenbezogene Daten der Rundfunkanstalt (z. B. sensible Gesundheitsdaten oder Recherchematerial aus dem investigativen Bereich) zu verarbeiten, so ist die Wahlmöglichkeit bezüglich der Betriebsmodelle eingeschränkt. Streng vertrauliche personenbezogene Daten müssen vollständig vor dem Zugriff Externer – einschließlich dem des externen Dienstleisters – geschützt sein, z. B. durch Ende-zu-Ende-Verschlüsselung. Dies gilt insbesondere für externe Dienstleister, die ihren Sitz außerhalb der EU haben und die Anforderungen der DSGVO nicht vollständig erfüllen können. Kann ein Zugriff des externen Dienstleisters nicht vollständig ausgeschlossen werden, so muss die Rundfunkanstalt ggf. im Verbund mit den anderen Rundfunkanstalten für diese streng vertraulichen personenbezogenen Daten ein eigenes System betreiben.

4. Auftragsverarbeitung

Entscheidet sich die Rundfunkanstalt für eine durch einen externen Dienstleister betriebene Kollaborationsplattform, so wird der Anbieter in datenschutzrechtlicher Hinsicht als Auftragsverarbeiter für sie tätig. Grundlage dafür ist ein Auftragsverarbeitungsvertrag, der die Anforderungen des Art. 28 DSGVO, insbesondere Abs. 3 lit. a) - g) DSGVO erfüllen muss. Abhängig vom Ergebnis der Schutzbedarfsfeststellung muss die Rundfunkanstalt angemessene technische und organisatorische Maßnahmen (TOM) zur Gewährleistung der Informationssicherheit vereinbaren bzw. ergreifen. Dazu gehören namentlich folgende Anforderungen an die Nutzung der Kollaborationsplattform:

- Ausschalten des Aktivitätstrackings von Teilnehmer*innen
- Möglichkeit für manuelle Datenschutzeinstellungen der Nutzer*innen entsprechend der internen Vorgaben der Rundfunkanstalt
- Transportverschlüsselung nach dem Stand der Technik
- Möglichkeit der Deaktivierung von Mitschnitten einer Videokonferenz und die Möglichkeit der Vorabinformation an die Teilnehmer*innen über die Aufzeichnung
- Automatische bzw. entsprechend den Aufbewahrungsbestimmungen festgelegte Löschung eventueller Aufzeichnungen bzw. Mitschnitte nach einer Videokonferenz
- Deaktivierung der Möglichkeit zur Erstellung von Nutzungsprofilen
- Möglichkeit einer Hintergrundweichzeichnung oder eines virtuellen Hintergrundes
- Nutzerbezogener Zugang mit sicherem Authentisierungsverfahren nach dem Stand der Technik; bei Zugriff außerhalb der Rundfunkanstalt Multi-Faktor-Authentifizierung

Sofern der Anbieter seinen Sitz in einem Nicht-EU-Staat hat bzw. die Daten in einem Nicht-EU-Staat verarbeitet, muss die Rundfunkanstalt überdies prüfen, ob die Datenübermittlung in das Drittland im Einklang mit den Art. 44 ff. DSGVO steht (Näheres dazu siehe Ziffer 3).

Außerdem muss die Rundfunkanstalt ausschließen, dass der Auftragsverarbeiter die beim Betrieb seiner Plattform verarbeiteten personenbezogenen Daten ohne ordnungsgemäße Einwilligung der jeweils Beteiligten bzw. ohne gesetzliche Grundlage für eigene Zweck nutzt.

III. Organisatorische Maßnahmen zur Einhaltung von Datenschutz und Informationssicherheit

In einem internen Regelwerk (Dienstanweisung, Betriebs- oder Dienstvereinbarung) sollte die Rundfunkanstalt die einzuhaltenden technischen und organisatorischen Maßnahmen (TOM) zur Gewährleistung von Datenschutz und Datensicherheit für die Administrator*innen und alle Anwender*innen verpflichtend festhalten. Zu den dort zu regelnden Punkten sollten insbesondere gehören:

- Überblick über die datenschutzrechtlichen Risiken bei der Nutzung von Kollaborationsplattformen (Information und Sensibilisierung)
- Freigabeverfahren, das festlegt, welche Kollaborationsplattformen für die Verarbeitung welcher Datenklassen freigegeben sind bzw. welche Voraussetzungen an die Freigabe gestellt sind

- datenschutzfreundliche Voreinstellungen (z. B. Kamera und Mikrofon deaktiviert) als vorgegebener Standard
- Vorgaben zum Funktionsumfang und zu Zugriffsberechtigungen, darunter etwa die Verpflichtung zur Prüfung, ob anstatt einer Video- eine Telefonkonferenz ausreicht, Einschränkungen bzw. Modalitäten zur Nutzung der Aufzeichnungsfunktion (Mittschnitt, Screenshot, Fotografie)
- Möglichkeit, den Zugang zu Konferenzen zu schützen (z. B. Registrierung, Passwort)
- Möglichkeit der Vorfilterung externer Teilnehmer*innen (z. B. virtueller Wartebereich für Gäste bzw. Externe)
- Geeignete und verlässliche Information aller Konferenzteilnehmer*innen über die Identität der Teilnehmer*innen
- Gewährleistung, dass alle personenbezogenen Daten nach Ablauf festgelegter Löschfristen effektiv gelöscht werden
- Ausschluss einer Auswertung der Daten zur Verhaltens- oder Leistungskontrolle.

IV. Dokumentation und Information

Die für den Einsatz der jeweiligen Kollaborationsplattform verantwortliche Rundfunkanstalt muss die Anwendung gemäß Art. 30 DSGVO in ihrem Verarbeitungsverzeichnis dokumentieren (Art. 5 Abs. 2 DSGVO) und außerdem ihre zur Nutzung des Systems berechtigten oder verpflichteten Beschäftigten über die mit dem Einsatz eines solchen Systems verbundenen datenschutzrelevanten Aspekte umfassend und verständlich informieren. In den Fällen, in denen die Datenverarbeitung via Kollaborationsplattform auf die Einwilligung der Beteiligten (etwa aus anderen Rundfunkanstalten oder sonstigen Organisationen) gestützt werden soll (Art. 6 Abs. 1 lit. a) DSGVO), muss die Rundfunkanstalt die Voraussetzungen zur Einholung einer rechtswirksamen Einwilligung schaffen. Im Falle einer Verletzung des Schutzes personenbezogener Daten beim Einsatz eines solchen Systems unterliegt die jeweils verantwortliche Rundfunkanstalt der Meldepflicht nach Art. 33 DSGVO.