Bundesanstalt
für den Digitalfunk der Behörden und
Organisationen mit Sicherheitsaufgaben

FAQs zum Datenschutz beim Videokonferenzsystem CMS-Bund Instanz

Sammlung der wichtigsten Fragen im Zusammenhang mit der DS-GVO und der CMS-Bund

Februar 2021

Version 1.0

Einleitung

Die nachstehenden Beiträge geben Antworten auf die wichtigsten Fragen zum Umgang der BDBOS mit dem Datenschutz beim Videokonferenzsystem CMS-Bund Instanz. Sie sollen es den Nutzerbehörden ermöglichen, den rechtmäßigen Umgang bei Benutzung des Videokonferenzsystems sicherzustellen.

Fragensammlung

Verarbeitung und Zweck

Welche personenbezogenen Daten werden verarbeitet?

Es werden die folgenden Kategorien personenbezogener Daten i.S.d. Art. 4 Nr. 1 DS-GVO verarbeitet:

Verkehrsdaten

Es handelt sich um Daten, die bei der Nutzung des Videokonferenzsystems entstehen. Dazu gehören immer die E-Mailadresse des Initiators sowie Beginn und das Ende der Verbindung. Zudem wird die Telefonnummer bei einer Einwahl per Telefon und die IP-Adressen der Nutzer verarbeitet. Bei einer Einwahl per Telefon ist die Telefonnummer als Benutzername in der Teilnehmerliste zu sehen.

Inhaltsdaten

Daten die bei der Nutzung des Videokonferenzsystems entstehen. Dies sind Bilder von den betroffenen Personen sowie vom Raum in dem sich die Personen aufhalten. Zudem können personenbezogene Daten durch die Kommunikation der Teilnehmer verarbeitet werden

Zu welchen Zwecken dürfen die Nutzerbehörden den Videokonferenzdienst verwenden?

Grundsätzlich liegt die Art der Nutzung des Videokonferenzdienstes in der Verantwortung der jeweiligen Nutzerbehörde. Sie muss sicherstellen, dass die Verarbeitung personenbezogener Daten auch gerechtfertigt ist.

Die BDBOS möchte es den Nutzerbehörden aber auch ermöglichen personenbezogene Daten mit einem hohen Schutzbedarf über CMS-Bund Instanz zu verarbeiten. Zu solchen Verarbeitungen kann es insbesondere Im Zusammenhang mit Bewerbungsgesprächen kommen. Um eine umfassende Nutzung zu ermöglichen befindet sich die BDBOS mit dem

BfDI im Austausch darüber, ob die Voraussetzungen für die Verarbeitung von Daten mit einem hohen Schutzniveau bereits erfüllt bzw. welche Anforderungen umzusetzen sind.

Verarbeitet die BDBOS personenbezogene Daten zu einem anderen Zweck, als zum Betrieb des Videokonferenzsystems?

Nein, eine Verarbeitung personenbezogener Daten zu einem anderen Zweck erfolgt nicht.

Werden personenbezogene Daten an Dritte weitergegeben?

Eine Weitergabe der personenbezogenen Daten an Dritte erfolgt grundsätzlich nicht. Die BDBOS stellt allein dem BSI personenbezogene Daten aufgrund von § 5 Abs. 1 S. 4 BSIG zur Verfügung. Diese werden jedoch zukünftig vor der Übermittlung anonymisiert.

Wie lange werden personenbezogene Daten durch die BDBOS gespeichert?

Verkehrsdaten (E-Mailadresse des Initiators einer Videokonferenz) werden für den Zeitraum der Videokonferenz gespeichert.

Die Kommunikationsinhalte werden nicht gespeichert, aufgezeichnet oder anderweitig verwendet.

Verkehrsdaten von Teilnehmern, die sich per WebRTC einwählen werden nicht gespeichert.

Verkehrsdaten von Teilnehmern, die sich nicht per WebRTC einwählen, werden in Form von CDR-Daten gespeichert. Die Speicherfrist beträgt standardisiert 30 Tage, soll aber zeitnah verkürzt werden.

Werden die Videokonferenzen aufgezeichnet oder anderweitig protokolliert?

Eine Aufzeichnung oder Protokollierung der Videokonferenzen erfolgt nicht.

Welchen Einfluss hat das Schrems II Urteil auf CMS-Bund Instanz?

Das Schrems II Urteil des EuGH (Rechtssache C-311/18) hat keinerlei Auswirkungen auf die Verarbeitung personenbezogener Daten beim Videokonferenzsystem CMS-Bund Instanz. Es erfolgen insbesondere keine automatisierten Datenabflüsse. Durch restriktive

Firewall-Regeln und Systemhärtung ist eine Kommunikation über unbekannte Ports nicht möglich.

Zudem ist eine automatisierte Herausgabe von Logdateien nicht vorgesehen. Zugriff auf Log-Daten erhalten Hersteller nur im vorher definierten und festgelegten Supportfall nach Freigabe durch die BDBOS und die Auftragsverarbeiterin.

Umsetzung der Betroffenenrechte

Wie werden die Betroffenenrechte durch die BDBOS sichergestellt?

Die BDBOS stellt die Rechte der betroffenen Personen folgendermaßen sicher:

- Das Recht auf **Auskunft (Art. 15 DS-GVO)** wird grundsätzlich über den User Help Desk der BDBOS sichergestellt. Dieser kann prüfen, ob eine konkrete IP-Adresse erfasst wurde und welche weiteren Verkehrsdaten damit verbunden sind. Zu Inhaltsdaten kann aufgrund der fehlenden Aufzeichnung keine Aussage getroffen werden. Mit der in Diskussion befindlichen Anonymisierung der Verkehrsdaten wird eine Auskunft zukünftig nicht mehr möglich sein.
- Bezüglich des Rechts auf **Berichtigung (Art. 16 DS-GVO)** wird aufgrund der aktuellen Ausgestaltung der Verarbeitung personenbezogener Daten kein Anwendungsbereich gesehen. Inhaltsdaten werden unmittelbar nach Ende der Konferenz gelöscht. Der Bildschirmname kann während einer laufenden Konferenz durch erneutes Beitreten zur Videokonferenz angepasst werden.
- Das **Recht auf Löschung (Art. 17 DS-GVO)** wird gewahrt, da die CMS-Bund Instanz Inhaltsdaten nur unmittelbar während der Konferenz verarbeitet („streamt“). Eine in CMS-Bund Instanz hinterlegte Funktion zur Aufnahme der Konferenz existiert nicht.
- Die Verkehrsdaten von Nutzern, die sich nicht über WebRTC einwählen, und von Anrufern werden standardisiert für 30 Tage gespeichert. Bezüglich einer Reduzierung der Speicherfristen befindet sich die BDBOS derzeit in der Umsetzung mit der Auftragsverarbeiterin.
- Für das Recht auf **Einschränkung der Verarbeitung (Art. 18 DS-GVO)** wird kein Anwendungsbereich gesehen, da eine Auswertung der Verkehrsdaten in Klarlage

nicht geplant ist und abseits von der Speicherung und der Verarbeitung zum Betrieb der Videokonferenz keine weitergehende Verarbeitung erfolgt.

- Für das Recht auf **Widerspruch nach Art 21 DS-GVO** wird nur ein begrenzter Anwendungsbereich gesehen, da abseits von der Verarbeitung für die Videokonferenz und die Übermittlung an das BSI keine Verarbeitung erfolgt, geht der Widerspruch ins Leere.

Welche Betroffenenrechte liegen in der Verantwortung der Nutzerbehörden?

Aus hiesiger Sicht sind alle weiteren, hier nicht aufgeführten Rechte der betroffenen Personen durch die Nutzerbehörden selbst zu gewährleisten. Darunter fällt auch die Umsetzung der Informationspflicht aus **Art. 13 und 14 DS-GVO**. Die BDBOS stellt hierzu eine gesonderte Datenschutzerklärung zur Verfügung.

Pflichten der Nutzerbehörden

Welche Belehrungspflichten obliegen den Nutzerbehörden?

Die Nutzerbehörden sind als datenschutzrechtlich Verantwortliche grundsätzlich dafür zuständig, über das Verbot des (gerade auch heimlichen) Mitschneidens von Video- und/oder Audiodaten, des Speicherns und des Verbreitens solcher Aufnahmen sowie dessen mögliche Strafbarkeit zu belehren.

Darüber hinaus sind die Nutzer darüber zu informieren, welche Privatsphäre-Einstellungen sie vornehmen können, um selbst auf den Schutz der personenbezogenen Daten hinzuwirken. Die BDBOS bietet dafür die nachfolgenden Möglichkeiten an:

- Der Nutzer hat die Möglichkeit sich selbst **ein Synonym** bei der Anmeldung zur Videokonferenz zu geben.
- Eine **Deaktivierung des Video- oder Mikrofonkanals** ist beim Beitritt oder auch während einer Videokonferenz jederzeit möglich.

Wie erfüllen die Nutzerbehörden die Informationspflichten gegenüber den betroffenen Personen?

Die Umsetzung der Informationspflichten aus Art. 13 und 14 DS-GVO obliegen grundsätzlich den Nutzerbehörden. Die BDBOS stellt hierzu eine Datenschutzinformation.

Wie ist mit Datenpannen umzugehen?

Die Meldepflichten aus Art. 33 und 34 DS-GVO obliegen grundsätzlich der jeweiligen Nutzerbehörde. Die BDBOS unterrichtet die Nutzerbehörde umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen die zwischen Nutzerbehörde und BDBOS geschlossene Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen.

Technische und organisatorische Maßnahmen

Welche technischen und organisatorischen Maßnahmen werden von der BDBOS ergriffen?

Der BDBOS werden über Ihre Auftragsverarbeiterin vertraglich technische und organisatorische Maßnahmen zugesichert. Diese sowie ergänzende Maßnahmen der BDBOS sind der Anlage 4 zur Musterauftragsverarbeitung zu entnehmen, die die BDBOS allen Nutzerbehörden zur Verfügung gestellt hat. Sollten technische und organisatorische Maßnahmen ergänzt werden, wird die BDBOS eine aktualisierte Liste zur Verfügung stellen.

Wie gewährleistet die BDBOS die Sicherheit der Übertragung?

Die Sicherheit der Datenübertragung wird zum einen durch eine https-Transportverschlüsselung sichergestellt. Bei Einwahl von öffentlichen Telefonnetzen erfolgt die Übergabe an das Konferenzsystem über eine gesicherte Verbindung der Telekom. Bei Einwahl von SIP- oder H.323-Endgeräten über das Internet besteht die Möglichkeit, wenn einer der Teilnehmer technisch nicht zu einer Verschlüsselung in der Lage ist, auf eine unverschlüsselte Verbindung zurückzufallen.

Die BDBOS unterbindet einen unbefugten Abfluss personenbezogener Daten durch die Platzierung des Systems im NdB-Rechenzentrum. Aufgrund fehlender Aufnahmefunktion ist ein systemseitiger Abfluss nicht möglich.

Wie wird sichergestellt, dass nur berechtigte Personen auf eine Videokonferenzsitzung und deren Daten zugreifen können?

Die Authentifizierung wird durch eine Einladung und einen Passwortschutz sichergestellt. Die Einladung enthält eine vom System vergebene Konferenz ID und ein dazugehöriges Passwort. Diese Informationen werden dem Buchenden zur Verfügung gestellt und an die berechtigten Teilnehmer übermittelt.

Es besteht die Möglichkeit durch den Buchenden die Konferenz ID und das Passwort getrennt und auf unterschiedlichen Wegen (Telefon, Skype oder E-Mail) an die berechtigten Teilnehmer zu übermitteln.

Ferner besteht die Möglichkeit, den Konferenzraum nach der Identitätsprüfung der anwesenden Mitglieder abzuschließen. Damit kann sichergestellt werden, dass keine unbefugten Personen an den Konferenzen teilnehmen.

Wie ist sichergestellt, dass technische Schwachstellen und sonstige Sicherheitslücken im Videokonferenzsystem in einem angemessenen Zeitraum behoben werden?

Es gibt vertraglich festgelegte Wartungsfenster. Es existiert darüber hinaus ein organisiertes Vorgehen für Patches. Um Schwachstellen zeitnah zu erkennen und zu beheben werden die Meldungen des CERT und der Hersteller aktuell bearbeitet und ein Schließen der Sicherheitslücken im Sinne des Servicevertrages erbracht.

Wo findet die Verarbeitung der Daten statt (wo stehen die Server und wo sitzen eventuelle Administratoren)?

Zur Gewährleistung des Datenschutzes erfolgt die Verarbeitung lediglich in Deutschland. Das System CMS-Bund Instanz steht im hochgesicherten Rechenzentrum der BDBOS. Eine Übermittlung an Drittländer ist ausgeschlossen und wird auch von der inländischen

Auftragsverarbeiterin der BDBOS auf Basis der Auftragsverarbeitungsvereinbarung sichergestellt.

Wie stellt die BDBOS die datenschutzrechtlichen Rahmenbedingungen Ihrer Beschäftigten (Telearbeit, Homeoffice etc.), die Zugriff auf die Nutzerdaten hätten, vor dem Hintergrund des Art. 9 DS-GVO sicher?

Ein Zugriff auf Art. 9 Daten durch die Beschäftigten erfolgt nicht, da Inhaltsdaten nur während der Konferenz verarbeitet werden. Es besteht seitens der Beschäftigten keine Möglichkeit zum Zugriff auf die Inhaltsdaten.

Impressum

Bundesanstalt
Für den Digitalfunk der Behörden und
Organisationen mit Sicherheitsaufgaben

Abteilung Steuerung/Konzeption
Kundenbetreuung SK2

Fehrbelliner Platz 3
10707 Berlin
Telefon: +49 30 18 681-45000 (Kundentelefon)
E-Mail: kundenbetreuung@bund.de
www.bdbos.bund.de

Bildnachweis: sdecoret – stock.adobe.com