Fraunhofer SIT

FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY

White Paper

AUSWAHL UND NUTZUNG WEBBASIERTER KOMMUNIKATIONSDIENSTE IN ZEITEN VON CORONA

Datenschutz und Datensicherheitsaspekte

Annika Selzer, Sarah Stummer, Ulrich Waldmann

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Impressum

Kontaktadresse
Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt

Telefon	06151 869-213
Telefax	06151 869-224
E-Mail	info@sit.fraunhofer.de
URL	www.sit.fraunhofer.de

Herausgeber
Fraunhofer-Institut für Sichere Informationstechnologie SIT

Bildquelle Umschlage
iStock.com/scyther5

Über das Fraunhofer-Institut für Sichere Informationstechnologie SIT

Das Fraunhofer-Institut für Sichere Informationstechnologie SIT zählt zu den weltweit führenden Forschungseinrichtungen für Cybersicherheit und Privatsphärenschutz. Das Institut beschäftigt sich mit den zentralen Sicherheitsherausforderungen in Wirtschaft, Verwaltung und Gesellschaft und betreibt praxisorientierte Spitzenforschung und Innovationsentwicklung. Zahlreiche Preise und Auszeichnungen belegen die hohe Qualität der Ergebnisse und Entwicklungen.

Die Wissenschaftlerinnen und Wissenschaftler des Instituts beschäftigen sich mit aktuellen Fragestellungen zu Cybersicherheit und Datenschutz und entwickeln in diesem Bereich neue Technologien und konkrete Lösungen für reale Herausforderungen. Das Institut unterstützt seine Partner etwa bei der Konzeption neuer IT-Systeme, dem Schutz von IT-Infrastrukturen sowie der Entwicklung neuer Produkte und Dienstleistungen. Gleichzeitig berät das Institut in wichtigen IT-Sicherheitsfragen und engagiert sich in der nationalen und internationalen Standardisierung.

Der Hauptsitz des Instituts befindet sich in Darmstadt. Darüber hinaus unterhält das Institut eine Niederlassung in St. Augustin bei Bonn und ein Büro in Berlin sowie in Mittweida. International ist das Institut in Israel und Singapur vertreten.

Über das nationale Forschungszentrum für angewandte Cybersicherheit ATHENE

Das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE ist eine Einrichtung der Fraunhofer-Gesellschaft für ihre beiden Darmstädter Institute SIT und IGD unter Beteiligung der Technischen Universität Darmstadt und der Hochschule Darmstadt.

ATHENE ist das europaweit größte Zentrum für angewandte Cybersicherheitsforschung. In einem bisher einzigartigen und innovativen Kooperationsmodell von universitärer und außeruniversitärer Forschung entwickelt ATHENE Sicherheitslösungen zum Wohl von Wirtschaft, Gesellschaft und Staat, berät regelmäßig Wirtschaft und öffentliche Verwaltung und unterstützt Firmengründer und Startups.

ATHENE arbeitet agil und effizient und kann so auch kurzfristig auf neue Herausforderungen und veränderte Bedrohungslagen reagieren.

Dieses Whitepaper wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Annika Selzer, Sarah Stummer, Ulrich Waldmann

Fraunhofer-Institut für Sichere Informationstechnologie, SIT
in Darmstadt.

Dieser Beitrag wurde durch den Informationssicherheits- und Datenschutzkoordinator der Fraunhofer-Gesellschaft Dr. Ulrich Pordesch unterstützt.

Inhalt

1 Problemstellung

Die Reise- und Kontaktbeschränkungen, die derzeit zur Eindämmung des Corona-Virus bestehen, stellen die Arbeitswelt vor neue Herausforderungen im Zusammenhang mit der Aufrechterhaltung der Kommunikations-, Vernetzungs- und Wissensvermittlungsmöglichkeiten. Unter anderem besteht in Zeiten von Corona ein erhöhter Bedarf am Einsatz von webbasierten Kommunikationsdiensten wie z. B. Webinar-, Videokonferenz- und Matchmaking-Diensten (nachfolgend zusammenfassend „Dienste" oder „webbasierte Dienste" genannt). Diese werden cloudbasiert als sogenannte Software-as-a-Service-Lösung angeboten und stellen Kommunikationsmittel für Online-Treffen bereit, um die derzeit geltenden Reise- und Kontaktbeschränkungen auszugleichen.

Bei der Auswahl und Nutzung solcher Dienste ist geltendes Datenschutzrecht zu beachten. Datenschutzrechtliche Vorschriften beziehen sich immer auf personenbezogene Daten, also Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. In der Arbeitswelt beziehen sich personenbezogene Daten in der Regel auf persönliche Angaben der eigenen Mitarbeitenden sowie der Kunden und sonstiger natürlicher Personen (im Folgenden zusammenfassend „Mitarbeitende und Kunden" genannt). Beispiele für personenbezogene Daten sind Namen, E-Mail-Adressen und Telefonnummern natürlicher Personen. Auch von natürlichen Personen genutzte Pseudonyme sind personenbezogene Daten.

Ziel des Datenschutzrechts ist es, die von einer Datenverarbeitung betroffenen Personen vor unbefugten und zu umfangreichen Verarbeitungen ihrer personenbezogenen Daten und damit möglicherweise einhergehenden Benachteiligungen zu schützen. Daher muss auch bei jeglicher Verarbeitung personenbezogener Daten in der Arbeitswelt geltendes Datenschutzrecht beachtet werden. Möchte ein Unternehmen also einen webbasierten Dienst einsetzen, etwa um in Zeiten von Corona die Kommunikationsmöglichkeiten der Mitarbeitenden aufrecht zu erhalten, so muss sichergestellt werden, dass der Dienst datenschutzkonform eingesetzt werden kann. Unter anderem gilt es die Notwendigkeit zum Abschluss von Auftragsverarbeitungsverträgen sowie ggf. die besonderen Anforderungen an die Datenverarbeitung in Staaten außerhalb des Europäischen Wirtschaftsraumes (sogenannte „Drittstaaten") zu beachten. Auch ist die Nutzung des Dienstes erst dann datenschutzkonform möglich, wenn die sorgfältige Auswahl des Dienstes dokumentiert wurde und die dienstnutzenden Personen über die Rahmenbedingungen der Datenverarbeitung informiert wurden.

Neben datenschutzrechtlichen Aspekten sind auch Datensicherheitsaspekte zu berücksichtigen. Datensicherheitsaspekte betreffen – anders als das Datenschutzrecht – nicht nur die Verarbeitung personenbezogener Daten, sondern aller Daten, die für ein Unternehmen schützenswert sind. Unter anderem sollte also auch die Sicherheit wettbewerbsrelevanter Angebote, vertraulicher Rezepturen und Patentanmeldungen durch Maßnahmen der Datensicherheit gewährleistet werden. Es ist daher z. B. wichtig zu beurteilen, ob vertrauliche Daten überhaupt im Rahmen der Nutzung eines webbasierten Dienstes verarbeitet werden sollten und ob die Daten geschützt werden sollten, etwa mit Hilfe eines geeigneten Verschlüsselungsverfahrens.

Der vorliegende Beitrag beschreibt Anforderungen des Datenschutzes und der Datensicherheit, um Unternehmen Handlungsfelder aufzuzeigen, die es bei der Auswahl webbasierter Dienste zu berücksichtigen gilt. Die wichtigsten Anforderungen sind am Ende des Beitrags in Form einer Checkliste zusammengefasst.

Die Nennung von Anforderungen im Hauptbeitrag und in der Checkliste erhebt keinen Anspruch auf Vollständigkeit. Es handelt sich ausdrücklich um eine *beispielhafte* Darstellung

wichtiger Anforderungen. Zu berücksichtigen ist auch, dass nicht jede der im Folgenden dargestellten Anforderungen in jedem Verarbeitungskontext gleich relevant ist. Des Weiteren ist zu beachten, dass das Datenschutzrecht für die Verarbeitung besonders sensibler personenbezogene Daten – wie z. B. Gesundheitsdaten oder Informationen zur religiösen oder politischen Überzeugungen einer Person – besonders hohe Anforderungen stellt. Sollen solche Daten verarbeitet werden, bestehen also ggf. weitere/strengere Anforderungen, als die im Folgenden dargestellten. Insofern ist auch zu bewerten, ob für den konkreten Verarbeitungskontext weitere, nicht im Folgenden vorgestellte Anforderungen berücksichtigt werden müssen.

2 Datenschutzaspekte

Ziel der folgenden Unterkapitel ist es, diejenigen Anforderungen vorzustellen, die in Bezug auf die Auswahl- und Nutzungsphase webbasierter Dienste *besonders wichtig* erscheinen.

Die Person, deren personenbezogene Daten durch ein Unternehmen oder eine sonstige Organisation verarbeitet werden, wird im Folgenden „betroffene Person" oder kurz „Betroffener" genannt. Das Unternehmen oder die sonstige Organisation, die die personenbezogenen Daten ihrer Mitarbeitenden und Kunden verarbeitet, wird im Folgenden „Verantwortlicher" genannt.

2.1 In der Auswahlphase zu berücksichtigende Aspekte

2.1.1 Datenschutz-Grundsätze

Das Datenschutzrecht regelt einige Grundprinzipien zum Schutz der von einer Datenverarbeitung betroffenen Personen. Diese Grundprinzipien werden auch als Datenschutz-Grundsätze bezeichnet. Sie regeln unter anderem Folgendes:

Personenbezogene Daten dürfen nur auf Basis einer bestehenden Rechtsgrundlage verarbeitet werden. Ob und welche Rechtsgrundlage für einen konkreten Verarbeitungskontext besteht, muss im Einzelfall geprüft werden. Bei der Nutzung webbasierter Dienste, die zur Aufrechterhaltung des Arbeitslebens und der Erfüllung der Arbeitsaufgaben *unbedingt erforderlich* sind, wird sich die Nutzung der Dienste durch die eigenen Mitarbeitenden vielfach mit der Durchführung des Arbeitsvertrages begründen lassen. Auch wenn die Dienstnutzung für die Erfüllung eines Vertrages mit einem Endkunden *unbedingt erforderlich* ist, wird sich die Datenverarbeitung häufig durch den mit dem Endkunden geschlossenen Vertrag legitimieren lassen. Eine weitere Möglichkeit der Legitimation einer Verarbeitung personenbezogener Daten ist z. B. *die informierte, zweckgebundene, eindeutig erteilte Einwilligung* des Betroffenen.

Der Umfang der verarbeiteten personenbezogenen Daten muss zudem auf das für den konkreten, vor Verarbeitungsbeginn festzulegenden Verarbeitungszweck erforderliche Maß beschränkt werden. So ist der Einsatz eines webbasierten Dienstes häufig gar nicht erforderlich, da stattdessen andere Dienste ausreichen, etwa anstelle von Diensten für Videokonferenzen solche für Telefonkonferenzen [Berl20]. Sind webbasierte Dienste jedoch erforderlich, ist bei deren Auswahl der (dienstbasiert verpflichtende) Umfang der verarbeiteten personenbezogenen Daten zu berücksichtigen und zu bewerten, ob die Datenverarbeitung im Rahmen der Dienstnutzung über das für den konkreten Verarbeitungszweck erforderliche Maß hinausgeht. Erhebt ein webbasierter Dienst für Videokonferenzen z. B. basierend auf der IP-Adresse einen – auch nur ungefähren – Standort des Betroffenen oder erfordert die Dienstnutzung durch Mitarbeitende die Angabe deren Privatanschriften, so sind diese Angaben in der Regel für die Nutzung eines Videokonferenzsystems nicht erforderlich, womit ggf. die Dienstnutzung nicht datenschutzkonform möglich wäre. Die Beschränkung des Umfangs personenbezogener Daten enthält darüber hinaus auch eine zeitliche Komponente, so dass personenbezogene Daten grundsätzlich zu löschen oder zu anonymisieren sind, wenn diese für die Zweckerreichung nicht mehr benötigt werden und keine gesetzlichen Mindestaufbewahrungspflichten einer Löschung im Wege stehen. Bei der Auswahl webbasierter Dienste ist insofern sicherzustellen, dass spätestens nach Beendigung der Dienstnutzung personenbezogene Daten durch den Dienstanbieter gelöscht werden. Da die betroffenen Personen in bestimmten Fällen auch das Recht haben, die Löschung ihrer personenbezogenen Daten durchzusetzen, sollte der Dienst auch die manuelle Löschung personenbezogener Daten durch den Verantwortlichen oder auch durch jeden einzelnen Betroffenen (bezogen auf dessen personenbezogene Daten) ermöglichen.

Darüber hinaus sind die personenbezogenen Daten durch Sicherheitsmaßnahmen vor unberechtigtem Zugriff, Manipulation und Verlust zu schützen. Insofern hat eine Prüfung zu erfolgen, ob der Dienstanbieter entsprechende Schutzmaßnahmen umgesetzt hat.[1]

2.1.2 Auftragsverarbeitung

Durch die Nutzung webbasierter Dienste erhält der Dienstanbieter in der Regel Zugriff auf personenbezogene Daten der Mitarbeitenden und/oder Kunden des Verantwortlichen, die sonst nur für den Verantwortlichen einsehbar wären. Um die Datenverarbeitung der Kunden- und Mitarbeiterdaten durch den Dienstanbieter zu legitimieren, muss der Verantwortliche in der Regel *verpflichtend* einen sogenannten Auftragsverarbeitungsvertrag mit dem Dienstanbieter schließen. Die Pflichtbestandteile eines solchen Vertrags sind rechtlich verbindlich festgelegt, unter anderem ist die Datenlöschung bei Auftragsbeendigung zu regeln.[2]

Viele Dienstanbieter haben einen solchen Vertrag bereits aufgesetzt, um ihn mit ihren Kunden abschließen zu können. In der Regel wird der Vertrag zusätzlich zum Rahmenvertrag der Dienstnutzung handschriftlich unterzeichnet. Einige Dienstanbieter „verstecken" die Pflichtbestandteile eines Auftragsverarbeitungsvertrages aber auch in ihrem Rahmenvertrag (teilweise leider auf den gesamten Vertrag verstreut) und sehen lediglich eine Bestätigung dieser Regelungen durch das Anklicken eines Buttons vor. Grundsätzlich kann der Auftragsverarbeitungsvertrag auch in dieser Form geschlossen werden, jedoch ist es für den Verantwortlichen schwieriger zu erkennen, bei welchen der Regeln es sich um die Pflichtbestandteile eines Auftragsverarbeitungsvertrages handelt und ob alle Pflichtbestandteile eines Auftragsverarbeitungsvertrages abgebildet werden.

Es ist sehr wichtig nachweisen zu können, dass der Auftragsverarbeitungsvertrag abgeschlossen wurde. Wird der Auftragsverarbeitungsvertrag ausschließlich durch eine online ausgeführte, bestätigende Handlung (Klicken eines Buttons) geschlossen, so sollte sich der Verantwortliche das Vertragswerk daher zur Dokumentation abspeichern und notieren, wann und wie er dem Vertragswerk zugestimmt hat. Ggf. kann auch ein Screenshot die Dokumentation unterstützen, sofern dem Verantwortlichen die Bestätigung des Vertragsschlusses angezeigt wird.

Sofern der Dienstanbieter kein Vertragsmuster für einen Auftragsverarbeitungsvertrag vorsieht und die Pflichtbestandteile des Auftragsverarbeitungsvertrages auch nicht Teil des Hauptvertrages sind, ist ein individueller Auftragsverarbeitungsvertrag auszuhandeln. Hilfestellungen dazu bietet unter anderem die "Formulierungshilfe Auftragsverarbeitungsvertrag".[3]

Für den Verantwortlichen ist es wichtig zu wissen, dass er aus datenschutzrechtlicher Sicht für die Datenverarbeitung beim Dienstanbieter weitestgehend verantwortlich bleibt. Insofern hat der Verantwortliche seinen Auftragsverarbeiter sorgfältig auszuwählen und diese Auswahl, inklusive der für die Auswahl entscheidenden Gründe, zu dokumentieren. Im Fokus der Auswahlentscheidung stehen die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen für die sichere Verarbeitung personenbezogener Daten. Diese sind auf Vollständigkeit und Angemessenheit zu überprüfen. Insbesondere können Zertifizierungen wichtige Anhaltspunkte für die Auswahl liefern. Sofern der Dienstanbieter nicht über

[1] Näher Ausführungen hierzu erfolgen in den nachfolgenden Kapiteln 2.1.2 und 3.

[2] S. hierzu auch wichtige Regelungsalternativen zur Löschung im Auftragsverarbeitungsvertrag, die im Kapitel 2.2.5 beschrieben sind.

[3] https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Formulierungshilfe-Auftragsverarbeitungsvertrag%20nach%20DSGVO_0.pdf.

einschlägige Zertifizierungen verfügt[4], können z. B. der Informationssicherheitsbeauftragte und/oder der betriebliche Datenschutzbeauftragte des Verantwortlichen die sorgfältige Auswahl unterstützen. Hierzu eignet sich insbesondere die Bewertung der durch den Auftragsverarbeiter getroffenen Schutzmaßnahmen. Grundlage für diese Bewertung kann die im Rahmen des Auftragsverarbeitungsvertrags verpflichtend aufzustellende Auflistung der technischen und organisatorischen Maßnahmen bilden.

Neben der sorgfältigen Auswahl in Bezug auf die technischen und organisatorischen Schutzmaßnahmen sollte der Verantwortliche insbesondere auch den „Gesamteindruck" zur Datenschutzfreundlichkeit des Dienstes und des Dienstanbieters einfließen lassen. Fordert die Dienstnutzung z. B. sehr viele, für den Zweck unnötige personenbezogene Daten oder beschreibt der Dienstanbieter in seinen Datenschutzinformationen sehr umfangreiche Datenweitergaben an Externe, so sollte die Dienstauswahl vor dem Hintergrund der datenschutzkonformen Nutzung kritisch hinterfragt werden. Auch wenn eine Recherche zum Dienst(anbieter) z. B. in der Vergangenheit erfolgte Datenschutz- oder Datensicherheitspannen aufdeckt, sollte die Dienstnutzung kritisch hinterfragt werden. Gegen die Auswahl eines Dienstanbieters spricht auch, wenn nicht sichergestellt werden kann, dass der Dienstanbieter die personenbezogenen Daten zu eigenen Zwecken verarbeitet [Berl20][5] oder der Dienstanbieter die Anforderungen an datenschutzfreundliche Voreinstellungen im Dienst nicht umsetzt.[6]

2.1.3 Drittstaatübermittlung

Sofern der Dienstanbieter die personenbezogenen Daten der Mitarbeitenden und Kunden des Verantwortlichen nicht ausschließlich innerhalb der EU oder den Staaten Norwegen, Liechtenstein, Island, Schweiz, Kanada, Israel, Japan, Jersey, Isle of Man, Guernsey, Uruguay, Andorra, Neuseeland, Färöer-Inseln und Argentinien[7] verarbeitet, muss er zusätzlich zum Abschluss eines Auftragsverarbeitungsvertrages Garantien für die Datenverarbeitung außerhalb dieser Staaten erbringen. Dies hat zum Hintergrund, dass innerhalb Europas und in den weiteren genannten Staaten ein gleichwertig hohes Datenschutzniveau sichergestellt wird, das Datenschutzniveau in anderen Staaten jedoch teilweise starken Schwankungen unterliegt.

Sofern ein US-amerikanischer Dienstanbieter dem EU-US-Privacy-Shield beigetreten ist, darf auch die Datenverarbeitung durch den US-amerikanischen Dienstanbieter ohne weitere Garantien erfolgen, bzw. stellt das EU-US-Privacy-Shield diese Garantie in Form einer Art Datenschutzselbstzertifizierung des jeweiligen beigetretenen Unternehmens dar. Es empfiehlt sich, den aktiven Status des Dienstanbieters abzurufen[8] und per Screenshot zu dokumentieren.

Sofern es sich nicht um einen US-amerikanischen Dienstanbieter handelt oder dieser nicht dem EU-US-Privacy-Shield beigetreten ist, können der Verantwortliche und der Auftragsverarbeiter die sogenannten EU-Standard-Datenschutzklauseln abschließen, um die geforderten Garantien zu erbringen. Die EU-Standard-Datenschutzklauseln sind ein von der Europäischen Kommission entwickeltes Vertragswerk,[9] das „künstlich" ein angemessenes Datenschutzniveau beim

---

[4] Vgl. hierzu Kapitel 3.7.

[5] Grundsätzlich schließt die Rolle des Auftragsverarbeiters die Verarbeitung der im Auftrag verarbeiteten Daten zu eigenen Zwecken aus. Bei Unsicherheiten sollte die Verarbeitung zu eigenen Zwecken über den Auftragsverarbeitungsvertrag ausgeschlossen werden.

[6] Mehr zum Thema im Kapitel 2.2.1.

[7] Das wichtigste Europäische Rahmengesetz für den Datenschutz schließt Datenverarbeitungen im Europäischen Wirtschaftsraum, also der EU sowie Liechtenstein, Island und Norwegen ein. Für die anderen aufgezählten Länder hat die Europäische Kommission entschieden, dass das dort geltende Datenschutzsystem mit dem Schutzniveau des Europäischen Datenschutzes vergleichbar ist.

[8] Dies ist unter folgendem Link möglich: https://www.privacyshield.gov/list.

[9] Der Vertrag für Datenübermittlungen an Auftragsverarbeiter in Drittstaaten ist abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087.

Auftragsverarbeiter sicherstellt. Dieses ist ohne inhaltliche Änderungen zu übernehmen und vom Verantwortlichen und Auftragsverarbeiter zu unterschreiben.

Setzt der Dienstanbieter selbst Auftragsverarbeiter ein – diese gelten dann als Unterauftragsverarbeiter – so beziehen sich die genannten Anforderungen auch auf die Unterauftragsverarbeiter, sofern sie ihren Sitz nicht innerhalb der EU und den o.g. weiteren Staaten haben [Berl20].

2.1.4 Mitbestimmungsrechte nach Betriebsverfassungsgesetz

Sollen in einem webbasierten Dienst auch personenbezogene Daten von Mitarbeitenden verarbeitet werden – was i.d.R. bereits durch die Nutzung des Dienstes durch Mitarbeitende gegeben ist – können sich im Zusammenhang mit der Einführung webbasierter Dienste Informations- und Mitbestimmungsrechte des Betriebsrates ergeben. Diese gilt es bei der Auswahl webbasierter Dienste zu berücksichtigen.

Grundsätzlich steht dem Betriebsrat ein allgemeines Mitwirkungsrecht zu. So hat er unter anderem über die Durchführung der zugunsten der Arbeitnehmer geltenden gesetzlichen, tariflichen und sich aus Betriebsvereinbarungen ergebenden Bestimmungen zu wachen. Hierzu gehören in erster Linie arbeitsrechtliche, aber auch datenschutzrechtliche Bestimmungen. [Alth18]

Neben dem allgemeinen Mitwirkungsrecht hat der Betriebsrat bei der Einführung und Anwendung von technischen Einrichtungen, die zur Verhaltens- oder Leistungskontrolle bestimmt sind, auch ein gesetzliches Mitbestimmungsrecht. Da es hierfür (entgegen dem Wortlaut „bestimmt sein“) ausreicht, dass die technische Einrichtung objektiv geeignet ist das Verhalten oder die Leistung der Beschäftigten zu kontrollieren und es unerheblich ist, ob die zur Verhaltens- oder Leistungskontrolle geeigneten Daten tatsächlich zu diesen Zwecken ausgewertet oder genutzt werden, [BuVo19] kommt dem Betriebsrat bei dem Einsatz von zahlreichen webbasierten Diensten ein Mitbestimmungsrecht zu. [MüPS20]

Um dem Betriebsrat die Wahrnehmung dieser Rechte zu ermöglichen, ist er rechtzeitig und umfassend sowie unter Angabe aller relevanter Informationen und Unterlagen, zu unterrichten.

Über die gesetzlichen Mitbestimmungspflichten hinaus können sich Rechte und Pflichten auch aus Kollektivvereinbarungen, wie Betriebsvereinbarungen ergeben.

2.2 Während der Nutzungsphase zu berücksichtigende Aspekte

2.2.1 Datenschutzfreundliche Voreinstellungen

Das Datenschutzrecht verpflichtet den Verantwortlichen auch dazu sicherzustellen, dass für seine Mitarbeitenden und Kunden die datenschutzfreundlichsten Einstellungen des Dienstes voreingestellt sind. Insbesondere ist in diesem Zusammenhang auch sicherzustellen, dass personenbezogene Daten durch datenschutzfreundliche Voreinstellungen nicht ohne Eingreifen des Betroffenen einer unbestimmten Zahl anderer Nutzer (oder sogar jedermann) zugänglich gemacht werden.

Hat der Verantwortliche auf die Voreinstellungen des Dienstes (durch eine fehlende Freigabe des Dienstanbieters) keinen Einfluss, und stellt der Dienstthersteller nicht selbst die datenschutzfreundlichste Voreinstellung ein, so kann der Dienst in der Regel nicht datenschutzkonform eingesetzt werden. Insofern ist die Möglichkeit der datenschutzfreundlichen Voreinstellung bereits in der Auswahlphase des Dienstes zu berücksichtigen.

2.2.2 Datenschutzinformation

Den Verantwortlichen trifft die Pflicht, die Betroffenen umfangreich über die äußeren Umstände der Datenverarbeitung im Zusammenhang mit der Dienstnutzung zu informieren. Diese Informationen sind dem Betroffenen unaufgefordert und in der Regel vor Beginn der Datenverarbeitung zur Verfügung zu stellen. Unter anderem hat der Verantwortliche die Betroffenen darüber zu informieren, wer der Verantwortliche ist und wie er kontaktiert werden kann, welche personenbezogenen Daten auf Basis welcher Rechtsgrundlage und zu welchen Zwecken verarbeitet werden, ob die Datenverarbeitung an einen Auftragsverarbeiter ausgelagert wird (ggf. in Staaten außerhalb Europas), welche Rechte den Betroffenen in Bezug auf die Datenverarbeitung zustehen und wann eine Löschung der personenbezogenen Daten erfolgt.

In Bezug auf die Dienstnutzung sollte den Betroffenen insbesondere auch aufgezeigt werden, welche ihrer personenbezogenen Daten für andere Nutzer des Dienstes einsehbar sind und wie lange sie einsehbar bleiben. Auch sollte der Webdienstanbieter als Auftragsverarbeiter konkret benannt werden und ggf. auch auf dessen Datenschutzinformationen hingewiesen werden.

Soll ein Dienst sowohl von Mitarbeitenden als auch von Kunden genutzt werden, muss bei der Darstellung der Verarbeitungszwecke und –rechtsgrundlagen ggf. zwischen den unterschiedlichen Personenkreisen unterschieden werden.

Wenn es dem Verantwortlichen nicht möglich ist, seine dienstspezifischen Datenschutzinformationen direkt auf der persönlichen Startseite/dem persönlichen Login seiner Mitarbeitenden und Kunden– gut sichtbar – vorzuhalten, so muss er andere Wege finden, seine Mitarbeitenden und Kunden vor Beginn der Datenverarbeitung zu informieren. An Mitarbeitende können die Informationen z. B. durch eine Rundmail verteilt werden. Auch für die Datenschutzinformation an Kunden ist dieser Weg denkbar, jedoch ist dabei zu beachten, dass eine gleichzeitige E-Mail an viele externe Teilnehmende unter Verwendung der „An" oder „CC"-Funktion der E-Mailprogramme zu einer Datenpanne führen kann, wenn die einzelnen Adressaten ihre Namen und E-Mailadressen vor dem E-Mailversand untereinander nicht kannten. Eine datenschutzkonforme Alternative kann der Versand unter Verwendung der „BCC"-Funktion sein.

2.2.3 Verbreitung von Ton- und Bildaufzeichnungen

Häufig sollen Termine, Webinare oder Schulungen, die mit einem webbasierten Dienst durchgeführt werden aufgezeichnet und verbreitet werden. In diesen Fällen sollte bereits bei der Auswahl des Dienstes berücksichtigt werden, dass entsprechende Funktionen möglichst datensparsam sind, etwa indem in Ton- und Bildaufnahmen die Namen der Teilnehmenden ausgeblendet werden können oder anstelle des Namens ein Pseudonym angezeigt wird (z. B. Teilnehmender 1). Grundsätzlich sollte vorgezogen werden, dass die Teilnehmenden in Aufnahmen nicht identifiziert werden können.[10]

Ist es jedoch gerade gewünscht, dass in der zu verbreitenden Ton- und Bildaufnahme alle Teilnehmenden identifiziert werden können oder lässt sich dies nicht vermeiden, erfordern die Aufnahme und Verbreitung der Ton- und Bildaufnahmen in der Regel eine datenschutzkonforme Einwilligung aller Teilnehmenden.[11]

---

[10] Dies bezieht sich lediglich auf die *Aufzeichnung* selbst. Dass die Teilnehmenden eines Webinars oder einer Videokonferenz untereinander wissen, wer sonst noch im „virtuellen Meetingraum" ist, ist i.d.R. aus Gründen der Transparenz des Informationsflusses wichtig und notwendig.

[11] Neben der Rechtsgrundlage sind auch die üblichen datenschutzrechtlichen Pflichten zu berücksichtigen. Dies betrifft insbesondere die Datenschutz-Grundsätze, welche in Kapitel 2.1.1 behandelt werden sowie die in Kapitel 2.2.2 erläuterte Datenschutzinformation.

Eine Einwilligung ist dann datenschutzkonform, wenn der Einwilligungstext verständlich, also in klarer und einfacher Sprache formuliert ist und der Zweck der Datenverarbeitung deutlich und konkret benannt wird. Auch ist es wichtig, dass die Einwilligung freiwillig abgegeben wird und die Betroffenen auf ihr Widerrufsrecht – das den Betroffenen verpflichtend zuzugestehen ist – hingewiesen wurden. Nicht zuletzt setzt eine datenschutzkonforme Einwilligung eine eindeutige, bestätigende Handlung voraus. Die Einholung der Einwilligung kann schriftlich, elektronisch und, sofern angemessen, auch mündlich erfolgen. Zu berücksichtigen ist hierbei die Pflicht des Verantwortlichen nachweisen zu können, dass von den Betroffenen Einwilligungen eingeholt wurden. Je nach Kontext bietet es sich daher an die Einwilligung elektronisch, etwa bei der Anmeldung zu einem Webinar oder bei der Einwahl in ein Webinar einzuholen.

Dem Veranstalter einer Videokonferenz/Schulung o.ä. ist darüber hinaus zu empfehlen, vor Beginn oder im Rahmen der Anmoderation des Termins die Teilnehmenden darauf hinzuweisen, dass auch sie nicht ohne Einwilligung Gespräche mitschneiden oder Fotos/Screenshots der Referierenden und Teilnehmenden anfertigen dürfen.

2.2.4 Datenpannen

Datenpannen sind Vorfälle, bei denen personenbezogene Daten externen, unberechtigten Stellen bekannt werden oder bekannt geworden sein *könnten.*[12] Wird dem Verantwortlichen im Zusammenhang mit der Dienstnutzung eine Datenpanne bekannt – z. B. weil es einem externen Hacker gelungen ist, Passworte der Dienstnutzer abzugreifen und darüber in der Presse berichtet wird und/oder der Dienstnutzer den Verantwortlichen über den Vorfall informiert – so hat der Verantwortliche zu bewerten, ob er die Datenpanne an die zuständige Datenschutz-Aufsichtsbehörde und ggf. sogar an die Betroffenen melden muss. Eine Meldung an die Aufsichtsbehörde muss binnen 72 Stunden nach Bekanntwerden der Datenpanne erfolgen und darf nur unterbleiben, wenn die Datenpanne voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Eine Benachrichtigung der betroffenen Person muss unverzüglich erfolgen, sofern die Datenpanne voraussichtlich zu einem hohen Risiko für deren Rechte und Freiheiten führt.

Dem Verantwortlichen ist zu raten, bereits vor einer Datenpanne festzulegen, wie im Falle einer Datenpanne zu verfahren ist. Wer bewertet, ob eine Meldung an die zuständige Aufsichtsbehörde und ggf. auch an die Betroffenen erfolgen muss? Wer übernimmt die Meldung? Wie wird sichergestellt, dass der interne Abstimmungsprozess nicht die zulässige Meldefrist von 72 Stunden überschreitet?

Je nach Schwere der Datenpanne sowie je nach Reaktion des Dienstanbieters auf die Datenpanne sollte der Verantwortliche darüber hinaus in Erwägung ziehen, den Dienstanbieter zu wechseln.

2.2.5 Datenlöschung

Wie bereits im Kapitel 2.1.1 dargestellt, sind personenbezogene Daten zu löschen, wenn sie für die Erbringung des Verarbeitungszwecks nicht mehr erforderlich sind. Spätestens bei Beendigung der Dienstnutzung durch den Verantwortlichen ist daher die Löschung der personenbezogenen Daten beim Dienstanbieter zu initiieren. In der Regel sieht der Auftragsverarbeitungsvertrag entweder die Option der Herausgabe der Daten an den Verantwortlichen oder aber die Löschung der Daten im Dienst vor. Hierfür kann laut Vertrag entweder der Auftragsverarbeiter oder aber – sofern dies im Dienst vorgesehen und freigegeben

[12] Solche Datenpannen verletzen das Schutzziel der Vertraulichkeit und sind im Zusammenhang mit webbasierten Diensten besonders relevant. Weitere Vorfälle können vorliegen, wenn die Schutzziele der Integrität oder der Verfügbarkeit verletzt werden. So liegt eine Verletzung der Verfügbarkeit z. B. vor, wenn über einen Dienst Informationen ausgetauscht werden, die nur in dem Dienst gespeichert werden und diese Daten verloren gehen.

ist – der Verantwortliche zuständig sein. Sofern der Auftragsverarbeiter für die Datenlöschung zuständig ist, sollte sich der Verantwortliche die Datenlöschung schriftlich bestätigen lassen.

Sofern einer Löschung gesetzliche Mindestaufbewahrungspflichten entgegenstehen – dies ist z. B. bei Daten der Fall, die zur Festlegung zu entrichtender Steuerabgaben notwendig sind – ist es notwendig, bereits im Auftragsverarbeitungsvertrag die Herausgabe der Daten bei Auftragsbeendigung zu regeln.

Auch der Auftragsverarbeiter selbst kann gesetzlichen Mindestaufbewahrungspflichten unterliegen. Soll der Auftragsverarbeiter bei Auftragsbeendigung alle Daten löschen und die Löschung bescheinigen, kann es daher vorkommen, dass der Auftragsverarbeiter unter Bezugnahme auf gesetzliche Aufbewahrungspflichten die Löschung bestimmter Daten aussetzt und diese nachholt, sobald die gesetzliche Aufbewahrungspflicht verstrichen ist. Auch dies sollte man sich schriftlich bestätigen lassen.

3 Datensicherheitsaspekte

3.1 Vertraulichkeit der Informationen

Unterschiedliche Informationen können eine unterschiedliche Sensitivität und damit einhergehende Schutzbedürftigkeit aufweisen. Daher gilt es bereits bei der Auswahl eines passenden webbasierten Dienstes zu prüfen, welche Daten und Informationen in dem Dienst verarbeitet werden sollen und wie vertraulich diese sind. Hiervon ist abhängig, ob die Nutzung eines Dienstes überhaupt zulässig ist und welche Risikobetrachtungen hierbei vorzunehmen sind. Zudem lassen sich an den Dienst zu stellende Anforderungen ableiten.

Hinsichtlich der Vertraulichkeit der Informationen ist insbesondere die Klassifizierung der zu verarbeitenden Informationen zu berücksichtigen. So sind öffentliche Informationen weniger schutzbedürftig als interne, welche wiederrum weniger Schutz erfordern als vertrauliche oder streng vertrauliche Informationen. Je höher die Vertraulichkeit der Informationen, desto höhere Schäden können für das Unternehmen entstehen. Demnach steigen die an einen Dienst zu stellenden Sicherheitsanforderung mit der Vertraulichkeit der Information. Einige Informationen dürfen aufgrund gesetzlicher oder vertraglicher Beschränkungen vielleicht auch gar nicht in einem webbasierten Dienst verarbeitet werden.

Neben den eigenen Unternehmensdaten können in webbasierten Diensten auch Daten von Vertragspartnern oder gemeinsam erarbeitete Betriebs- und Geschäftsgeheimnisse verarbeitet werden – häufig auch auf Wunsch des Vertragspartners. Solche Vorhaben können vertraglichen Beschränkungen unterliegen und daher vertraglich unzulässig sein.[13] Zudem können die betroffenen Informationen Vertraulichkeitsvereinbarungen unterliegen, gegen welche durch eine Übermittlung solcher geschützten Daten verstoßen werden könnte. Bevor Daten von Vertragspartnern in webbasierten Diensten verarbeitet werden, sollte daher geprüft werden, ob diese Daten Vertraulichkeitsvereinbarungen unterliegen. Soll ein webbasierter Dienst auf Wunsch des Vertragspartners trotz der Vertraulichkeitsvereinbarung eingesetzt werden, sollte hierfür vorab eine schriftliche Zustimmung eines bevollmächtigten Vertreters des Vertragspartners eingeholt werden. Im Übrigen sollte von einer Nutzung der durch eine Vertraulichkeitsvereinbarung geschützten Daten eines Vertragspartners in webbasierten Diensten abgesehen werden.

3.2 Länderspezifische Besonderheiten

Werden webbasierte Dienste mit Kunden oder im Rahmen von Projekten genutzt, sollte geprüft werden, ob hinsichtlich der im Webdienst übermittelten Daten oder der beteiligten Unternehmen und Mitarbeitenden ein erhöhtes länderspezifisches Risiko besteht. So sollte beispielsweise vermieden werden, Daten über webbasierte Dienste zu übermitteln, die diese Daten in einem Land außerhalb des europäischen Rechtsraums verarbeiten, dessen Gesetze möglicherweise nicht bekannt sind oder bekanntermaßen weniger mit der europäischen Rechtsauffassung übereinstimmen. Beispielsweise könnte im ungünstigen Fall ein Zugriff durch Sicherheitsbehörden auf übermittelte Daten die betreffenden Kunden oder Projektpartner sogar persönlich gefährden.

Allerdings kann auch bei einer Datenverarbeitung in der EU nicht ausgeschlossen werden, dass Anbieter (insbesondere solche, die ihren Hauptsitz außerhalb der EU haben) in bestimmten Fällen von Gerichten oder nationalen Sicherheitsbehörden gezwungen werden, Daten an Behörden herauszugeben. Die Datenverarbeitung in Rechenzentren der EU oder sogar lokal im

[13] Vgl. Kapitel 4.2.

eigenen Unternehmen sind aber gegenüber behördlichen Datenzugriffen u. U. besser geschützt, auch in der Hinsicht, dass eine Information der Betroffenen oder ein Widerspruch vor Gericht in der EU eher möglich sind.

3.3 Verschlüsselung

Ein wichtiges Kriterium für die Sicherheit eines webbasierten Dienstes ist die verschlüsselte Übertragung der Daten. Der Dienst sollte bei der Datenübertragung Verschlüsselungsverfahren nach dem Stand der Technik einsetzen, mindestens eine Verschlüsselung der Kommunikationskanäle mit TLS 1.2. Diese sogenannte Transportverschlüsselung bietet gewisse Sicherheit, dass unbeteiligte Dritte die Daten auf dem Übertragungsweg nicht mitlesen können. Beim Einsatz von Serverzertifikaten für TLS kann überprüft werden, dass sich die Teilnehmenden des Online-Meetings tatsächlich mit dem gewünschten Webdienst verbinden und nicht etwa mit einem gefakten Server kommunizieren. Auf den Servern des Anbieters liegen die Daten allerdings zumindest kurzzeitig unverschlüsselt vor, so dass der Anbieter darauf zugreifen kann. Der Anbieter bekommt auch viele technische Daten der Kommunikation mit, beispielsweise Informationen über die Geräte der Nutzer, wenn die Kommunikation cloudbasiert über einen Server des Anbieters vermittelt wird.

Gerade in Bezug auf die eingesetzten Sicherheitsverfahren ist es aufschlussreich, die Webseiten des Anbieters zu besuchen und ggf. die dort veröffentlichten technischen Angaben zu prüfen. Existieren beispielsweise Whitepaper, die der Dienst und die darunterliegende Technik einigermaßen plausibel beschreiben? Werden darin Begriffe erläutert und nicht einfach nur marketingorientiert genutzt? Häufig verwenden Anbieter den Begriff "Ende-zu-Ende-Verschlüsselung", ohne die "Enden" der Kommunikation klar zu benennen. Das dem Nutzer gegenüberliegende Ende ist meist ein Server des Anbieters. Dort liegen die Daten dann unverschlüsselt vor, gerade auch um den Nutzern besondere Funktionen wie die Aufzeichnung eines Online-Meetings anzubieten. Dagegen meint echte Ende-zu-Ende-Verschlüsselung die Verschlüsselung und Entschlüsselung ausschließlich auf Seiten der Nutzer (in den Client-Geräten), um eine durchgehende Verschlüsselung von Nutzer zu Nutzer zu garantieren. Diese kann dann nicht mehr vom Anbieter mitgelesen werden. Eine notwendige Voraussetzung dazu ist allerdings, dass individuelle Schlüssel im Client-Programm der einzelnen Nutzer erzeugt werden und diese Schlüssel die Geräte der Nutzer niemals verlassen. Nur dann haben die Dienstanbieter keine Möglichkeit, die Daten zu entschlüsseln.

Ende-zu-Ende-Verschlüsselung ist bei Videokonferenzsystemen in der Regel nicht realisiert. Selbst wenn webbasierte Dienste die Daten über den Transportweg hinaus verschlüsseln (beispielsweise die verschlüsselte Speicherung einer Konferenz anbieten), werden die Schlüssel meist auf dem Server des Anbieters erzeugt und kontrolliert. Auch beim Angebot einer Verschlüsselung der Dateninhalte bekommen häufig alle Teilnehmenden denselben Schlüssel, weil es sehr aufwändig (und zeitkritisch) wäre, die Daten zwischen den Teilnehmenden umzuverschlüsseln. Zudem wäre die Benutzungsfreundlichkeit, z. B. von beliebigen Geräten auf die Daten zuzugreifen, wahrscheinlich herabgesetzt. Eine absolute Sicherheit gegen Zugriffe des Dienstes und Betreibers kann daher nicht bestehen.

3.4 Aspekte der Installation

Bei der Auswahl eines geeigneten Dienstes lassen sich einige Sicherheitsrisiken vermeiden. So sollte der Dienst möglichst ohne Installation von Zusatzkomponenten wie Browser-Plugins oder Webserver auf den Geräten der Endnutzer auskommen, damit keine zusätzlichen Sicherheitsrisiken (z. B. Installation von Schadsoftware) entstehen. Reine Webanwendungen, z. B. auf Grundlage des offenen Standards WebRTC ohne Installation zusätzlicher Komponenten, erheben zudem meist weniger Daten als installierte Client-Software oder Smartphone-Apps.

Außerdem ist es den Mitarbeitenden und Vertragspartnern, die in verschiedenen Projekten eingebunden sind, nicht immer zuzumuten, für jedes Projekt für die Kommunikation ggf. eine andere Client-Software zu installieren. Zudem starten viele Client-Programme automatisch und belegen Peripheriegeräte wie Kamera und Mikrofon, so dass ein Zugriff durch ein anderes, gerade benötigtes Client-Programm möglicherweise verhindert wird.

Andererseits können auch Webanwendungen wie WebRTC sicherheitstechnische Nachteile haben. Denn dem Browser müssen dazu weitgehende Rechte einräumt werden, zumindest den Zugriff auf Kamera und Mikrofon. Ob der Browser diese Rechte auf die entsprechende Session begrenzt oder ob Anwendungen in anderen Browser-Fenstern oder zu einem späteren Zeitpunkt diese Rechte ebenfalls nutzen können, hängt von der Güte der Browser-Implementierung ab. Für die Nutzer ist das schwierig zu überprüfen. Eine separat installierte Client-Software beansprucht zwar meist noch mehr Rechte als eine Anwendung im Browser; dafür können diese Rechte aber nicht von einer anderen Software missbraucht werden.

Eine Entscheidung über Webanwendung oder Client-Installation sollte besser im Einzelfall und aus der Perspektive der zukünftigen Nutzer getroffen werden: Soll die Kommunikationslösung langfristig für eine feste Benutzergruppe (z. B. interne Mitarbeitende des Unternehmens) zum Einsatz kommen, dann spricht vieles für die Installation von Client-Software. Soll die Lösung dagegen nur vereinzelt in der Kommunikation mit externen Projektpartnern oder Kunden (z. B. in Webinaren) verwendet werden, können die Vorteile einer reinen Webanwendung überwiegen, für die die Kommunikationspartner nur auf einen Weblink klicken müssen.

In jedem Fall gilt die Bereitstellung des Dienstes durch einen Server vor Ort, der vom Unternehmen für seine Mitarbeitenden und Projektpartner selbst betrieben wird, als sicherer und datenschutzfreundlicher im Vergleich zur Nutzung von Cloud-Lösungen externer Anbieter, da lokale Datenflüsse besser kontrolliert werden können und die Daten mit höherer Wahrscheinlichkeit innerhalb der eigenen Organisation bleiben. Garantiert ist das jedoch nicht. Denn die Hersteller und Software-Anbieter könnten dennoch Daten aus der laufenden Nutzung ihres Produktes erheben (insbesondere technische Diagnosedaten für die Produktentwicklung) und auch während der Nutzung des Dienstes im Browser Daten für eigene Zwecke erheben und an Dritte weiterleiten. Sicherheits- und Datenschutzvorfälle und Diskussionen über die Vertrauenswürdigkeit des Produkts sind ggf. im Internet auffindbar.

3.5 Kommunikationsstandards

Weitere Kriterien zur Einschätzung der Sicherheit sind: Werden die eingesetzten Kommunikationsschnittstellen und Netzwerkprotokolle benannt? Handelt es sich dabei um bekannte und öffentlich einsehbare Standards? Gibt es dokumentierte Programmier-schnittstellen (APIs), die auch von anderen Herstellern verwendet werden können? Das kann als Hinweis gedeutet werden, dass keine geheimen Datenabflüsse stattfinden. Anerkannte Verfahren einschließlich der empfohlenen Schlüssellängen und Konfiguration sind meist gut dokumentiert, beispielsweise in den technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Eine zweckfremde Weiterleitung von Daten an den Anbieter kann mit hoher Wahrscheinlichkeit bei Open-Source-Lösungen ausgeschlossen werden, weil deren Programmcode einsehbar ist und oftmals von unabhängigen interessierten Personen und IT-Experten auf „Hintertüren“ überprüft wurde.

Verwendet die webbasierte Lösung stattdessen proprietäre Schnittstellen und unbekannte Ver-schlüsselungsverfahren, dann sind die Zusagen des Anbieters meist nicht von außen überprüfbar. Selbstverständlich können auch offene Standards und empfohlene Verschlüsselungsverfahren falsch implementiert und falsch konfiguriert sein. Doch ist die Wahrscheinlichkeit, dass Sicherheitsmängel in öffentlich einsehbaren Spezifikationen und

Programmcodes entdeckt und beseitigt werden, viel höher als bei einem proprietären Verfahren eines einzelnen Anbieters.

3.6 Sicherheitskonzept

Die IT-Abteilung des Unternehmens und die Verantwortlichen auf Leitungsebene müssen darüber informiert werden, welche webbasierte Kommunikationslösung eingesetzt werden soll. Zunächst sollte geklärt werden, ob für einen Dienst die vorhandene Infrastruktur um Server, Netze, Hardware und Software erweitert werden muss. Notwendige Zusatzkomponenten sollten möglicherweise in einem Sicherheitskonzept berücksichtigt werden, weil sie auch andere Teile der IT-Infrastruktur gefährden können. Evtl. müssen IT-Netze zusätzlich abgesichert, Clients und Server für die neue Lösung speziell konfiguriert werden. Zudem muss später auf evtl. auftretende Datenschutz- und Sicherheitsvorfälle schnell und angemessen reagiert werden können, siehe Unterkapitel 2.2.4.

Die Verantwortlichen müssen die Risiken für die Sicherheit der Daten abwägen und für angemessene Sicherheitsmaßnahmen sorgen. Wichtige Fragen in diesem Zusammenhang sind:

- Besteht aufgrund technischer und organisatorischer Randbedingungen ein erhöhtes Risiko für Sicherheitsvorfälle?
- Wird durch den Dienst die Wahrscheinlichkeit von Angriffen erhöht?
- Kommen durch den Dienst neue und innovative Technologien zum Einsatz?

Neue Technologien verwenden häufig proprietäre Protokolle und benötigen evtl. eine hohe externe Konnektivität und die Kontrolle durch einen externen Dienstleister. Die Sicherheit kann auch durch hohes Datenvolumen gefährdet sein. Die Konsequenzen und Sicherheitsmängel der neuen Technologie sind evtl. noch unbekannt.

Die Klärung dieser Fragen ist Teil einer Risikoabschätzung, die dokumentiert werden sollte. Die zu treffenden Sicherheitsmaßnahmen sollten auf Leitungsebene abgestimmt und in Form eines separaten Sicherheitskonzepts oder durch Erweiterung bestehender Konzepte dokumentiert werden. Diese Dokumentation muss die datenschutzrelevanten kritischen Eigenschaften des Dienstes berücksichtigen, z. B. auch den Fall, dass der webbasierte Dienst eine besondere Form der Datenverarbeitung (z. B. KI, Machine Learning, Sprach-, Sprecher- oder auch Gesichtserkennung) verwendet.[14]

Das Sicherheitskonzept muss klar beschreiben, welche Verschlüsselungs- und Authentisierungsverfahren lokal an den Client-Geräten der Nutzer sowie ggf. zentral an den Servern zum Einsatz kommen, ob eine lokale Datenspeicherung stattfindet (z. B. Aufzeichnung von Konferenzen, Protokollierung der Nutzung, Backups) und wie ggf. der Zugriff auf diese gespeicherten Daten geregelt ist. Spezielle Sicherheitsmaßnahmen sollten ebenfalls im Konzept beschrieben sein. Dazu können die Standards ISO 27002 und ISO 27701 Orientierungshilfe geben, insbesondere für Maßnahmen der Zugriffskontrolle wie das Registrieren und Austragen von Nutzern sowie den Einsatz kryptografischer Verfahren. Schließlich muss definiert sein, wie die Einhaltung der Sicherheitsmaßnahmen über die gesamte Nutzungsphase des Dienstes organisatorisch und technisch überprüft wird.

[14] Im Falle des Einsatzes neuer Technologien ist aus Datenschutzsicht zudem über die Notwendigkeit der Durchführung einer sogenannten „Datenschutz-Folgenabschätzung" zu entscheiden. Die Datenschutz-Folgenabschätzung ist ein Instrument des Datenschutzrechts, mit dem Risiken für die Betroffenen und das Risiko eindämmende Schutzmaßnahmen systematisch erhoben werden. Sie ist in einige Fällen – unter anderem wenn sehr viele besonders sensible personenbezogene Daten verarbeitet werden sollen oder wenn neue Technologien zum Einsatz kommen – verpflichtend durchzuführen. Mehr zur Datenschutz-Folgenabschätzung unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf.

3.7 IT-Sicherheitszertifizierungen

Allgemein sollten webbasierte Dienste bevorzugt werden, deren Anbieter in ihrem Erscheinungsbild seriös und möglichst nachvollziehbar Wert auf IT-Sicherheit und Vertraulichkeit legen. Eine IT-Sicherheitszertifizierung des Anbieters, beispielsweise nach ISO 27001 und ISO 27018, oder die Zertifizierung eines Produkts nach den Common Criteria gemäß ISO 15408, evtl. sogar durch eine vom BSI anerkannte Prüfstelle, geben Hinweise darauf, dass der Anbieter ausreichende Angaben zum Schutz der Daten gemacht und seine Prozesse und Sicherheitsmaßnahmen gut dokumentiert hat. Ein solcher Anbieter ist wahrscheinlich schon länger bekannt und relativ seriös.

Für Unternehmen und Nutzer ist es allerdings meist aufwändig und schwierig, die Bedeutung und den Umfang einer IT-Sicherheitszertifizierung einzuschätzen, die ein Anbieter für seine Dienste beansprucht. Beispielsweise sind evtl. nur kleine, unbedeutende Bereiche eines Dienstes zertifiziert oder der Anbieter macht pauschale Angaben ("ISO-zertifiziert"), ohne klärende Details zu nennen. Zudem werden Zertifikate immer nur für einen begrenzten Zeitraum ausgestellt. Ein behauptetes Zertifikat kann also bereits veraltet sein. Für aktuelle Informationen sollte unbedingt auch die offizielle Webseite der jeweiligen Zertifizierung als Referenz herangezogen werden, weil dort in der Regel die ausgestellten Zertifikate und teilweise auch Auszüge aus den Prüfberichten veröffentlicht sind.

Eine fehlende Zertifizierung bedeutet nicht, dass ein webbasierter Dienst als unsicher gelten muss. Denn eine Zertifizierung kostet viel Zeit und Geld, die bei kleineren Anbietern oder in einem dynamischen Umfeld (neue Technologien, Open Source, Gemeinschaftsprojekt) oftmals nicht vorhanden sind. Letztlich können jede Neuerung und jedes Update eine bestehende Produktzertifizierung wieder in Frage stellen.

3.8 Kenntnis über den Nutzerkreis

Die moderierende Person und alle Teilnehmenden eines geplanten Online-Meetings sollten unbedingt vorab den vollständigen Teilnehmerkreis kennen, um gut einschätzen zu können, welche Inhalte besprochen werden können. Die Teilnahme an einem Meeting sollte in jedem Fall nur nach einer erfolgreichen Authentisierung möglich sein. Bei einer unternehmensinternen Installation des Dienstes sollte es möglich sein, für unterschiedliche Teilnehmergruppen auch unterschiedliche Profile einzurichten. So wäre beispielsweise für ein internes Meeting von Teilnehmenden einer Organisation ein Verbindungsaufbau über eine Authentisierung mit einem personengebundenen Nutzerkonto (Passwort, Smartcard) angemessen, d.h. eine Teilnahmebeschränkung auf einzelne Nutzerkonten des Unternehmens. Erfolgt die Teilnehmerverwaltung innerhalb eines installierten webbasierten Dienstes, so muss diese mit dem Verzeichnisdienst des Unternehmens abgestimmt sein.

Für Gruppen mit externen Personen sollte ebenfalls der Teilnehmerkreis festgelegt sein. Eine anonyme Teilnahme darf nicht möglich sein, auch wenn unter den Teilnehmenden Pseudonyme genutzt werden. Einige Dienste sehen eine Registrierung mit Name und E-Mail-Adresse vor, an die ein Aktivierungslink gesendet wird. Wenn der Zutritt in ein Online-Meeting durch Eingabe eines Passworts erfolgt, dann sollte die moderierende Person das Passwort idealerweise unabhängig von der Einladung verteilen. Der versendete Weblink auf das Meeting sollte jedenfalls nicht allein schon den Zugang zum Meeting ermöglichen, auch wenn dies als besonders nutzungsfreundlich empfunden werden könnte. Bei Teilnehmenden, die nicht vorab registriert wurden, sollte der Dienst zusätzlich zum Klick auf den Weblink die Eingabe eines Passworts von jeder teilnehmenden Person erfordern. Zudem ist die Nutzung kurzer Konferenz-IDs in den Weblinks aus Sicherheitssicht bedenklich, da kurze IDs von Angreifern erraten und für eine unberechtigte Teilnahme missbraucht werden können. Je länger (z. B. 20 Zeichen) und

zufälliger (gemischt aus Ziffern, Buchstaben, Sonderzeichen) die vom Dienst automatisch generierten IDs sind, desto besser.

4 Sonstige relevante Aspekte

4.1 Freigabe der Dienstnutzung und Vertragsschluss

Die Nutzung webbasierter Dienste ist mit vielfältigen Implikationen verbunden, die den einzelnen Mitarbeitenden eines Unternehmens meist nicht vollständig bekannt sein können. Mitarbeitende sollten nicht allein über den Einsatz eines webbasierten Dienstes entscheiden. In jedem Fall sind über den geplanten Einsatz eines webbasierten Dienstes immer erst die jeweiligen Vorgesetzten zu informieren. Bei Projektkooperationen sollte geprüft werden, ob der Kooperationsvertrag eine solche Verwendung erlaubt. Schließlich sollte der webbasierte Dienst nur nach eingehender Prüfung durch die Verantwortlichen offiziell im Unternehmen zur Nutzung freigeben werden.

Da durch die Beschaffung oder die Nutzung des webbasierten Dienstes ein Vertrag zwischen dem Dienstanbieter und dem Unternehmen entsteht und häufig interne Richtlinien (z. B. Einkaufs- oder Unterschriftenrichtlinien) bestehen, die den Abschluss von Verträgen bestimmten Personenkreisen vorbehalten, ist zudem zu berücksichtigen, ob die jeweils den Vertrag abschließende Person dazu berechtigt ist, Verträge im Namen des Unternehmens abzuschließen und damit die vertraglichen Bedingungen für das Unternehmen als verbindlich zu akzeptieren. Zu prüfen ist daher, ob eine bloße Freigabe der Dienstnutzung durch den Vorgesetzten ausreichend ist und ob nicht weitere interne Richtlinien zu berücksichtigen sind.

In Einzelfällen kann anstelle eines Vertrags zwischen dem Dienstanbieter und dem Unternehmen auch ein Vertrag zwischen dem Dienstanbieter und der den Vertrag abschließenden Person als Privatperson zustande kommen. Hierbei ist zu prüfen, ob die private Mitbenutzung eines solchen privat beschafften Dienstes im Unternehmens-Kontext gestattet ist. Zudem ist zu berücksichtigen, ob der Dienst für Unternehmenszwecke genutzt werden darf.[15]

4.2 Vertragliche Zulässigkeit der Dienstnutzung

Vor der Nutzung webbasierter Dienste sollte unbedingt geprüft werden, ob dies im jeweiligen Kontext vertraglich zulässig ist, denn die Nutzung von Dienstleistern und Unterauftragnehmern kann (z. B. durch einen Vertrag mit einem Dienstleister oder Kunden) vertraglich ausgeschlossen oder die Nutzung webbasierter Dienste beschränkt sein.

Zu prüfen ist daher, ob ein Vertrag Klauseln enthält, die den Einsatz von Unterauftragnehmern, Dienstleistern oder die Nutzung von webbasierten Diensten generell ausschließen. Liegt eine vertragliche Beschränkung vor und soll ein webbasierter Dienst entgegen der vertraglichen Vereinbarung genutzt werden oder wünscht der Vertragspartner die Nutzung eines solchen Dienstes entgegen der vertraglichen Vereinbarung, sollte von dem jeweiligen Vertragspartner vor Beginn der Nutzung des Dienstes eine Zustimmung eingeholt werden. Da eine solche Zustimmung regelmäßig eine Vertragsänderung darstellt und Verträge für eine solche häufig die Schriftform erfordern, sind hierbei mögliche sich aus dem Vertrag ergebende Formerfordernisse für Vertragsänderungen zu berücksichtigen. Zudem ist zu berücksichtigen, dass die Zustimmung durch einen bevollmächtigten Vertreter des Vertragspartners eingeholt wird.

Besteht hinsichtlich möglicher vertraglicher Beschränkungen Unsicherheit, sollte ebenso eine entsprechende Zustimmung eingeholt werden. So lassen sich Vertragsverstöße und daraus folgende Ansprüche des Vertragspartners vermeiden.

[15] Vgl. hierzu Kapitel 4.3.

Häufig wird anstelle eines pauschalen Verbots von Unterauftragnehmern, Dienstleistern oder dem Einsatz von webbasierten Diensten auch ein Zustimmungsvorbehalt des Vertragspartners oder jedenfalls eine Pflicht zur Information des Vertragspartners vereinbart. Entsprechend sollte geprüft werden, ob der Einsatz webbasierter Dienste vertraglich an bestimmte Bedingungen geknüpft ist.[16]

4.3 Gesamtbild „Nutzungsbedingungen“

Die Nutzung webbasierter Dienste ist stets an vertragliche Rahmenbedingungen, wie z. B. die einzuhaltenden Nutzungsbedingungen geknüpft. Für die Nutzung eines Dienstes für betriebliche Zwecke können diese Nutzungsbedingungen jedoch häufig ungeeignet oder sehr einschneidend sein. Daher gilt es bei der Auswahl eines Dienstes die Nutzungsbedingungen kritisch zu prüfen und diese bei der Nutzung zu berücksichtigen.

Eine Regelung, die häufig in Nutzungsbedingungen kostenfreier Dienste zu finden ist bestimmt, dass der Dienst einzig zu privaten Zwecken genutzt werden darf. Folglich stellte die Nutzung des Dienstes zu betrieblichen Zwecken einen Verstoß gegen die Nutzungsbedingungen dar, welcher negative Rechtsfolgen habenkönnte. In diesem Fall sollte auf einen anderen Dienst oder, sofern vorhanden und für betriebliche Zwecke gestattet, die kostenpflichtige Version des Dienstes ausgewichen werden.

Eine weitere Regelung, die einige Nutzungsbedingungen vorsehen, bestimmt, dass der Betreiber des Dienstes bestimmte Nutzungsrechte eingeräumt bekommt. Dies könnte z. B. Rechte an der über den Dienst erfolgten Kommunikation oder an den im Dienst eingestellten Daten und Informationen betreffen. Schwere Folgen für das Unternehmen kann dies insbesondere haben, wenn über den Dienst Betriebs- oder Geschäftsgeheimnisse ausgetauscht werden. Sind Daten von Vertragspartnern oder Ergebnisse eines Auftrags betroffen, können die Folgen über das Unternehmen hinaus auch Vertragspartner betreffen. So können etwa Verwertungsmöglichkeiten des Vertragspartners verloren gehen.

Ob eine entsprechende Einräumung AGB-rechtlich wirksam ist, ist im Einzelfall oft unklar, insbesondere auch vor dem Hintergrund, dass ausländisches Recht zu berücksichtigen sein kann. Aus diesem Grund sowie um Rechtsstreitigkeiten insgesamt vorzubeugen, sollten entsprechende Regelungen bereits vor Beginn der Nutzung des Dienstes bekannt sein. Auf diese Weise kann verhindert werden, dass ungewollt Nutzungsrechte eingeräumt werden, oder es kann auf einen anderen Dienst ausgewichen werden.

Eine weitere kritische Regelung, die in einigen Nutzungsbedingungen zu finden ist könnte der Vorbehalt zur Datenweitergabe, etwa bei Firmenverkauf darstellen. Je nach Gegenstand der ausgetauschten Informationen und Daten sowie je nach Empfänger der Daten kann ein solcher Vorbehalt unerwünschte Folgen haben, weshalb entsprechende Regelungen bereits vor Beginn der Nutzung bekannt sein sollten.

Aufgrund der zuvor dargestellten möglichen Regelungen in Nutzungsbedingungen, aber auch aufgrund einer Vielzahl von weiteren nachteiligen Regelungen, die Nutzungsbedingungen enthalten könnten sollten die Nutzungsbedingungen von einzusetzenden Diensten unbedingt vor deren Nutzung kritisch geprüft werden.

[16] Zu berücksichtigen sind auch mögliche Vertraulichkeitsvereinbarungen, vgl. hierzu Kapitel 3.1.

4.4 (Interne) Nutzungsrichtlinien

Die Geeignetheit webbasierter Dienste hängt immer auch vom Nutzungsverhalten der Anwendenden ab. So kann ein Dienst alle der zuvor dargestellten Anforderungen erfüllen; wird er nicht richtig genutzt, können dennoch Risiken für die Nutzenden, das Unternehmen oder die Vertragspartner entstehen. Daher sollte das Unternehmen Nutzungsrichtlinien verfassen, in denen dargestellt wird, welche Maßnahmen zu treffen sind und wie der Dienst genutzt werden soll.

Grundsätzlich hängen die in diesen Nutzungsrichtlinien konkret abgebildeten Maßnahmen von den Anforderungen des jeweiligen Unternehmens und dem webbasierten Tool ab. Mögliche Maßnahmen können jedoch unter anderem folgende sein:

- Regelmäßige Änderung des Passworts eines Konferenzraumes
- Verwendung Konferenz-individueller Passwörter
- Vergabe persönlicher Passwörter für jede teilnehmende Person
- Verbergen von Konferenz-Metadaten wie Meeting-ID oder Veranstalter-PIN
- Einschalten des Wartebereichs, d. h. Deaktivieren der Option "Beitritt vor Gastgeber ermöglichen".
- Standardmäßiges Stummschalten und Video-Aus beim Eintritt von Teilnehmenden. Die Freigabe zur Nutzung von Mikrofon und Kamera sollte beim Eintritt in eine Konferenz abgefragt werden und nie einseitig durch den Moderator der Veranstaltung (oder gar andere Teilnehmende) aktivierbar sein.
- Einlassen der einzelnen Teilnehmenden nur durch die moderierende Person
- Abschließen des Konferenzraums durch die moderierende Person, sobald alle gewünschten Teilnehmenden anwesend sind.
- Standardmäßiges Einblenden der Teilnehmerliste zur Kontrolle auf unberechtigte Teilnehmende.
- Einblenden der Mikrofon- und Kamera-Aktivitäten der Teilnehmenden
- Teilen des Bildschirms nur durch die moderierende Person und durch diejenigen Personen, denen sie dieses Recht gewährt und wieder entzieht.

  Deaktivieren von Aufzeichnen der Konferenz durch die Teilnehmenden oder zumindest Kontrolle darüber durch die moderierende Person.
- Deaktivieren weiterer nicht-genutzter Konferenzmechanismen
- Aktives Beenden der Konferenz durch die moderierende Person. Der Dienst sollte dann automatisch alle Verbindungen beenden.

Zusätzlich zu diesen Maßnahmen sollten die Nutzungsrichtlinien Hinweise zur Nutzung und damit verbundenen „Dos and Don'ts" enthalten. Auch diese sind abhängig von dem Dienst und den jeweiligen Anforderungen. Beispiele für Hinweise könnten jedoch sein, dass der Termin und die Zugangsdaten einer Online-Konferenz nicht in Kalendern, Foren, sozialen Netzwerken oder Webseiten bekannt gemacht werden, welche von Personen außerhalb des Teilnehmerkreises gelesen werden können und dass eine rechtzeitige Ankündigung der Einladung und das Versenden der Einladung/Zugangsdaten erst kurz vor dem Termin nützlich sein könnten. Zudem könnte darauf hingewiesen werden, dass die Teilnehmenden bis zum Eintritt der moderierenden Person in einem Wartebereich verbleiben sollten, von dem sie ausschließlich durch die

moderierende Person in das Meeting eingelassen werden. Falls es sich um eine Videokonferenz handelt, könnte weiterhin darauf hingewiesen werden, dass andere Kanäle, wie reine Sprachkanäle (z. B. Einwahl über Telefon) ausgeschlossen werden, da diese die Erkennung der Teilnehmenden erschweren.

5 Zusammenfassende Checkliste

5.1 In der Auswahlphase zu berücksichtigende Aspekte

- Bitte prüfen Sie, ob anstelle eines webbasierten Dienstes ein anderer Dienst ausreichend ist (z. B. Telefonkonferenz anstelle von Videokonferenz); *Details ab S. 11.*
- Bitte prüfen Sie, ob eine Rechtsgrundlage für die Verarbeitung im Rahmen der Dienstnutzung besteht (z. B. eine Einwilligung) und im Rahmen des Dienstes nur unbedingt erforderliche personenbezogene Daten verarbeitet werden (wie z. B. der Name, nicht aber der Standort der Nutzer); *Details auf S. 11.*
- Bitte prüfen Sie, ob der Dienstnutzung Regelungen aus Kollektivvereinbarungen (z. B. Betriebsvereinbarungen) oder Verträgen (z. B. NDAs) entgegenstehen und/oder der Betriebsrat die Dienstnutzung erlauben muss; *Details auf S. 14.*
- Bitte prüfen Sie, ob Sie mit dem Dienstanbieter einen Auftragsverarbeitungsvertrag schließen müssen und ob der Dienstanbieter in einem „Drittstaat" außerhalb der EU ansässig ist, für den zusätzlich zum Auftragsverarbeitungsvertrag weitere Garantien wie z. B. ein Beitritt zum EU-US-Privacy-Shield oder unterzeichnete EU-Standard-Datenschutzklauseln vorliegen müssen; *Details ab S. 12.*
- Bitte überprüfen Sie den Dienstanbieter u.a. in Bezug auf die von ihm vorgegebenen Nutzungsbedingungen und Datenschutzinformationen, die im Dienst ermöglichten Datenschutz-Einstellungen (z. B. zur Löschung) und die vom Dienstanbieter getroffenen technischen und organisatorischen Maßnahmen (letzteres z. B. auf Basis von IT-Sicherheitszertifizierungen wie ISO 27001 und ISO 27018, Common Criteria gemäß ISO 15408); *Details insb. auf den S. 12, 14, 23.*
- Bitte prüfen Sie, ob durch den Dienst neue und innovative Technologien (z. B. KI, Sprach- , Sprecher- und Gesichtserkennung) zum Einsatz kommen und bewerten Sie ggf. die Notwendigkeit einer Datenschutz-Folgenabschätzung; *Details auf S. 22.*
- Bitte prüfen Sie, ob länderspezifische Risiken einer Dienstnutzung entgegenstehen (z. B. Vermeiden der Übermittlung landespolitisch kritischer Inhalte mittels Webdienst eines Dienstanbieters des betreffenden Landes); *Details ab S. 19.*

5.2 Während der Nutzungsphase zu berücksichtigende Aspekte

- Bitte prüfen Sie, ob die datenschutzfreundlichsten Einstellungen des Dienstes (z. B. in Bezug auf die externe Sichtbarkeit der Nutzer und darauf, dass Kamera und Mikrofon zunächst standardmäßig ausgeschaltet sind) voreingestellt sind; *Details auf den S. 14, 27.*
- Bitte erfüllen Sie Ihre Informationspflichten (z. B. durch den Versand einer Datenschutz-erklärung im Rahmen der Einladung zu einer Videokonferenz); *Details ab S. 15.*
- Bitte sorgen Sie für einen kontrollierten Zugang zu virtuellen Konferenzräumen (z. B. durch vorausgehende Registrierung der Teilnehmenden oder Eingabe eines Passwortes) und ändern Sie ggf. regelmäßig das Passwort eines wiederholt genutzten virtuellen Konferenzraumes; *Details insb. auf den S. 23, 27.*
- Bitte fertigen Sie ohne die Zustimmung der teilnehmenden Personen keine Ton- und Bildaufnahmen an (z. B. Aufzeichnung eines Webinars, um den Mitschnitt im Anschluss auf der Unternehmenswebseite zu veröffentlichen). Weisen Sie zu Beginn einer Veranstaltung auch die Teilnehmenden darauf hin, dass diese keine Screenshots, Fotografien oder Ähnliches anfertigen dürfen, ohne zuvor die Einwilligung der anderen Teilnehmenden und der Referierenden einzuholen; *Details ab S. 15.*
- Bitte prüfen Sie spätestens bei Beendigung der Dienstnutzung, wie im Dienst gespeicherte personenbezogene Daten gelöscht werden (z. B. manuell durch die Nutzer oder automatisch durch Sie oder den Dienstanbieter); *Details ab S. 17.*

6 Literatur

6.1 Verwendete Literatur

[Alth18] Althoff, Lars; Die Rolle des Betriebsrats im Zusammenhang mit der EU-Datenschutzgrundverordnung, ArbRAktuell 2018, 414.

[Berl20] Berliner Beauftragte für Datenschutz und Informationsfreiheit; Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Checkliste_Videokonferenzen.pdf, 15. April 2020.

[BuVo19] von dem Bussche, Dr. Axel Freiherr/Voigt, Paul; Konzerndatenschutz, 2. Auflage, C.H. Beck, München 2019.

[MüPS20] Müller-Glöge, Dr. Rudi/Preis, Dr. Dr. h.c. Ulrich/Schmidt, Ingrid, Erfurter Kommentar zum Arbeitsrecht, 20. Auflage, C.H. Beck, München 2020.

6.2 Zum Weiterlesen

Bundesamt für Sicherheit in der Informationstechnik (BSI): Kompendium Videokonferenzsysteme, KoViKo - Version 1.0.1, April 2020: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm

DSK, Kurzpapier zu Auftragsverarbeitung: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

DSK, Kurzpapier zur Datenübermittlung in Drittstaaten: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf

DSK, Kurzpapier zur Einwilligungen nach der DS-GVO: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf

DSK, Kurzpapier zu den Informationspflichten bei Direkt- und Dritterhebung: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf

DSK, Kurzpapier zur Datenschutz-Folgenabschätzung: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf

Gesellschaft für Datenschutz und Datensicherheit e.V.; GDD-Praxishilfe DS-GVO XVI - Videokonferenzen und Datenschutz, April 2020: https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_xvi-videokonferenzen-und-datenschutz

Fraunhofer-Institut
für Sichere Informationstechnologie

Rheinstraße 75 ·64295 Darmstadt
www.sit.fraunhofer.de