DZ CompliancePartner

Datenschutz in einer virtuellen Jahreshauptversammlung

Die Corona-Notfallgesetzgebung betrifft auch die Jahreshauptversammlung. Mit Blick auf die Kontakteinschränkungen und vor dem Hintergrund eines generellen Veranstaltungsverbots ist die virtuelle Hauptversammlung eine viel diskutierte Alternative. Dieser Leitfaden gibt einen Überblick der zu beachtenden datenschutzrechtlichen Aspekte.

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken

Jahreshauptversammlung 2020

Die hauptversammlungsrelevanten Regelungen der Corona-Notfallgesetzgebung sind am 28.03.2020 in Kraft getreten.

Unternehmen, deren Jahreshauptversammlung bevorsteht, sollten prüfen, inwieweit eine virtuelle Jahreshauptversammlung für sie in Betracht kommt. Oder ob sie diese auf einen späteren Zeitpunkt im Jahr verschieben, um sie – sofern dann wieder möglich – als Präsenzveranstaltung abzuhalten.
Solange die deutschlandweit geltenden behördlichen Verfügungen Veranstaltungen unabhängig von der Teilnehmerzahl untersagen, hilft allerdings nur eine virtuelle Jahreshauptversammlung.

Diese Möglichkeit wird nun erstmals gesetzlich geschaffen. Der Vorstand darf mit Zustimmung des Aufsichtsrats entscheiden, dass die Jahreshauptversammlung ohne physische Präsenz der Mitglieder oder Aktionärsvertreter virtuell durchgeführt wird.

Hierzu müssen jedoch neben technischen Herausforderungen auch rechtliche Anforderungen, etwa die der Datenschutz-Grundverordnung (DSGVO) bewältigt werden.

Corona-Notfallgesetzgebung
Die für die Durchführung einer Jahreshauptversammlung relevanten Regelungen sind im Internet abrufbar: https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/2020/1-quartal/corona-gesetzespaket-im-bundesrat.html.

Abgrenzung

In diesem Leitfaden wird ausdrücklich nur auf datenschutzrelevante Aspekte der virtuellen Jahreshauptversammlung eingegangen. Sonstige rechtliche Fragen sollten mit der Rechtsabteilung oder externen Rechtsanwälten beraten werden.

Videokonferenzsysteme und Cloud-Lösungen

Nutzung von Videokonferenzsystemen

Eine naheliegende Möglichkeit zur Durchführung einer virtuellen Jahreshauptversammlung sind Videokonferenzsysteme oder auf gleichen Technologien beruhende Lösungen.

Grundsätzlich können Videokonferenzen sowohl mit zwei als auch mit mehreren Teilnehmern durchgeführt werden. Auch in modernen Lösungen spiegelt sich diese Unterscheidung noch oft in den Anforderungen an die zugrundeliegende Technik wider. Bei manchen Lösungen sind bis heute unterschiedliche Anwendungsprogramme erforderlich.

Zu den klassischen Leistungsmerkmalen zählen
- die Echtzeit-Übertragung von Audio- und Videodaten der Teilnehmer
- die Darstellung des eigenen Video-Bildes sowie
- die Möglichkeit der reinen Audio-Teilnahme über eine klassische Telefonverbindung.

Durch die Planung der Konferenzen werden meist automatisch auch die notwendigen Konferenzressourcen geprüft und reserviert. Hierdurch können etwaige Kapazitätsengpässe schon im Vorfeld einer Konferenz erkannt und vermieden werden.

Neben den geplanten, temporären Videokonferenzen können den Nutzern dauerhaft persönliche „Virtuelle Konferenzräume“ zugewiesen werden. Diese Konferenzräume stehen dann den Nutzern jederzeit zur Verfügung, um mit weiteren Teilnehmern zu kommunizieren. Außerdem können Nutzer ad-hoc Konferenzen mit weiteren Teilnehmern innerhalb und außerhalb der Institution initiieren.

Cloud-Lösungen

Die Tendenz zu IT-Diensten aus der Cloud kann insbesondere auch bei Lösungen für die virtuelle Jahreshauptversammlung ein möglicher Lösungsansatz sein. Viele Anbieter von Videokonferenzlösungen haben zudem Dienste aus der Cloud im Angebot.

Videokonferenzsysteme
Einen Überblick der unterschiedlichen Anwendungsprogramme gibt das BSI Kompendium Videokonferenzsysteme, KoViKo - Version 1.0.1, im Internet:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf?__blob=publicationFile&v=4

Eine Multipoint Control Unit als zentrale Komponente einer Videokonferenzlösung in der Cloud bietet viele Möglichkeiten, die eine On-Premises-Variante (lokale Lösung) nicht leisten kann. Ein wichtiger Punkt ist die Skalierbarkeit. Oft bieten solche Angebote den Vorteil, dass Nutzer diese Systeme über einen Webbrowser nutzen können. Bei dieser Variante sind allerdings zusätzliche Datenschutzkontrollen beim Dienstleister erforderlich. Hier muss neben dem Konferenzsystem auch das Rechenzentrum auf seine Sicherheit überprüft werden.

Die mobile Nutzung von Videokonferenzlösungen erfolgt in der Regel unter ungünstigeren Bedingungen als die stationäre Nutzung am Arbeitsplatz oder in einem Besprechungsraum. Die Gründe dafür können sein:
- die Kameras, Mikrofone und Displays, die auf mobilen Geräten wie zum Beispiel Laptops, Tablets oder Smartphones zur Verfügung stehen
- die eingeschränkten Netzverbindungen einer mobilen Nutzung. Dabei werden häufig Verbindungen über ein WLAN oder Mobilfunknetz zum Internet und von dort aus zur Videokonferenzlösung aufgebaut. Hierbei steht gegebenenfalls nur eine geringe Bandbreite zur Verfügung, sodass die Bild- und Sprachqualität reduziert wird.

Zudem ist bei der mobilen Nutzung typischerweise die Umgebung des mobilen Teilnehmers nicht unter Kontrolle der Institution, sodass Bildbearbeitungstechniken zum Ausblenden des Hintergrundes an Bedeutung gewinnen. Diese müssen auf ihre Risiken hin überprüft werden. Gegebenenfalls sind entsprechende Schutzmaßnahmen einzurichten.

1. Verarbeitung personenbezogener Daten

Im Rahmen der virtuellen Jahreshauptversammlungen werden über eine Videokonferenzlösung als auch durch weitere Dienste vielfältige Daten gespeichert.

Dazu zählen insbesondere die folgenden Daten:
- Konfigurationsdaten der Komponenten
- Benutzerdaten
- Protokolldaten zu durchgeführten Videokonferenzen (typische Metadaten)
- (persistente) Chat-Nachrichten
- Dateien, die von den Nutzern in einer Dateiablage gespeichert werden
- Aufzeichnungen von Videokonferenzen.

Vielfach werden dabei personenbezogene Daten gespeichert. Dies trifft insbesondere auf Verbindungsinformationen sowie sämtliche nutzerbezogenen Daten zu.

Die Speicherung der Daten kann in Abhängigkeit der Architektur und der jeweiligen Komponente, die die Daten speichert, innerhalb der Videokonferenzlösung oder mittels externer Dienste und Speicherorte geschehen. Dabei kann es sich bei den Datensätzen sowohl um flüchtige Daten, die nur während einer Konferenz gespeichert werden, als auch um persistente, d. h. dauerhaft gespeicherte Daten handeln.

Zudem sind bei virtuellen Jahreshauptversammlungen rechtliche Fragestellungen, die sich auf die Durchführung sowie die Abstimmung beziehen, von erheblicher Relevanz.

Rechtliche Herausforderungen beim Abstimmungsverhalten und Fragen durch Teilnehmer

Im Rahmen der Jahreshauptversammlung besteht neben der Option einer Vollmachterteilung auch die Option einer elektronischen Kommunikation. Hierbei sind jedoch besondere Herausforderungen des Datenschutzes und der Informationssicherheit zu beachten.

Das ist z. B. bei der Nutzung eines Online-Formulars oder ähnlicher, digitaler Eingabemöglichkeiten relevant. Und es gilt vor allem auch in Bezug auf das Fragerecht der Teilnehmer. Denn auch bei einer elektronischen Kommunikation muss die Möglichkeit bestehen, im Rahmen der Hauptverhandlung Fragen zu stellen. Der völlige Ausschluss des Fragerechts ist nicht zulässig.

Im Gegensatz zu einer „analogen" Jahreshauptversammlung liegt schon beim Stellen einer Frage eine Verarbeitung von personenbezogenen Daten im Sinne der DSGVO vor, da die Frage digital übertragen wird. Daraus ergeben sich entsprechende Herausforderungen.

Mit Blick auf eine datenschutzsichere Durchführung stellt insbesondere der Spagat zwischen
- verpflichtender Nachweisbarkeit, etwa der Anwesenheit, aber auch gestellter Fragen und
- bestehenden Ansprüchen auf Anonymität, etwa bei geheimen Wahlen

hohe Anforderungen an die einzusetzende Technologie.

2. Einhaltung der Datenschutzgrundsätze

Die Datenschutzgrundsätze dienen als allgemeine fundamentale Regeln, die anderen Regeln zugrunde liegen. Diese Grundprinzipien des Datenschutzes ergeben sich aus Art. 5 Abs. 1 DSGVO.

Die Grundsätze für die Verarbeitung personenbezogener Daten ergeben sich als Antworten auf die Frage, welche Bedingungen bei der Verarbeitung personenbezogener Daten gegeben sein müssen, um Datenschutz und informationelle Selbstbestimmung zu gewährleisten.

Die Grundsätze beschreiben rechtlich erwünschte Zustände, die in der Verwirklichung des Rechts zu erreichen sind.

Sie enthalten somit Zielsetzungen für die Gestaltung der Datenverarbeitungssysteme und die Durchführung der Datenverarbeitungsvorgänge. Diese Zielsetzungen können je nach Inhalt unterschiedlich klare Grenzen angeben, ob sie erreicht worden sind oder nicht.

Es muss also im Rahmen der virtuellen Jahreshauptversammlung darauf geachtet werden, dass diese Grundsätze gewährleistet sind, namentlich die

- Rechtmäßigkeit,
- Verarbeitung nach Treu und Glauben,
- Erfüllung der Anforderungen an die Transparenz,
- Zweckbindung der erhobenen Daten,
- Datenminimierung,
- Garantie der Richtigkeit der Daten,
- Speicherbegrenzung sowie die
- Integrität und Vertraulichkeit der Daten.

Hinzu kommt, dass gem. Art. 5 Abs. 2 DSGVO die Einhaltung dieser Grundsätze durch eine schriftliche Dokumentierung vom Verantwortlichen nachgewiesen können werden muss. Bereits ein Verstoß gegen diese Rechenschaftspflicht kann zu Bußgeldern in Höhe von bis zu 20 Millionen Euro oder 4 % des Jahresumsatzes des gesamten Unternehmens führen.

3. Einhaltung der Betroffenenrechte

Im Rahmen der virtuellen Jahreshauptversammlung ist auch darauf zu achten, dass die Rechte der betroffenen Personen gewahrt werden.

Betroffenenrechte regeln das Recht der von der Datenverarbeitung betroffenen Personen. Den betroffenen Personen stehen im Vorfeld, während und nach der Datenverarbeitung zahlreiche Rechte zu Verfügung. Der Verantwortliche muss diese Rechte gewähren und ist insoweit in der Regel zu einer unverzüglichen Reaktion verpflichtet. Längstens darf die Reaktionsfrist jedoch nicht über einem Monat liegen.

Folgende Aspekte sind zwingend zu berücksichtigen:

- Transparente und vollumfängliche Hinweise gem. Art 13/14 DSGVO vor Beginn der virtuellen Jahreshauptversammlung
- Erfüllung von Auskunftsansprüchen gem. Art 15 DSGVO
- Gegebenenfalls die Berichtigung oder Löschung falscher Informationen gem. Art 16 - 18 DSGVO
- Möglicherweise die Erfüllung des Anspruchs auf Datenübertragbarkeit gem. Art 20 DSGVO.

4. Abschluss eines Vertrages

Die DSGVO setzt bei der Auslagerung von Aufgaben im Rahmen der Auftragsverarbeitung eine vertragliche Grundlage für die Verarbeitung dieser Daten voraus.

Eine Auslagerung an IT-Dienstleister ermöglicht es, sich auf das Kerngeschäft zu konzentrieren und Fehler bei den Datenverarbeitungsprozessen zu vermeiden. Zugleich eröffnen sich erhebliche Chancen für Dienstleister, deren Geschäftsmodell die professionelle Erbringung derartiger Prozesse ist.

Es ist zu gewährleisten, dass die Anforderungen des Art. 28 DSGVO erfüllt sind und dies gem. Art. 28 Abs. 3 in einem entsprechenden Vertrag festgelegt wird. Im Rahmen dieser Vereinbarung müssen auch technische und organisatorische Maßnahmen festgelegt, dokumentiert und überprüft werden.

5. Auswahl und Kontrolle des Dienstleisters

Art. 28 DSGVO setzt voraus, dass der Verantwortliche nur mit Auftragsverarbeitern zusammenarbeitet, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass der Schutz der Rechte der betroffenen Person gewährleistet ist.

Damit legt der Gesetzgeber dem Auftraggeber die indirekte Pflicht auf, den Auftragnehmer sorgfältig auszuwählen.

Insofern muss sich der Verantwortliche, sowohl vor Beginn der Datenverarbeitung (Erstkontrolle) als auch regelmäßig im laufenden Betrieb von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen überzeugen. z. B. durch Bewertung von erneuerten Zertifikaten.

Zu solchen Kontrollen gehört insbesondere die Prüfung der nachfolgenden Anforderungen:

Bestehen Maßnahmen zur Verwehrung des Zutritt zu Gebäuden, in denen die Verarbeitung durchgeführt wird, für Unbefugte?	❑
Bestehen Maßnahmen zur Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte?	❑
Bestehen Maßnahmen zur Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern?	❑
Bestehen Maßnahmen zur Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten?	❑
Bestehen Maßnahmen zur Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte?	❑
Bestehen Maßnahmen zur Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben?	❑
Bestehen Maßnahmen zur Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können?	❑
Bestehen Maßnahmen zur Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind?	❑
Bestehen Maßnahmen zur Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden?	❑
Bestehen Maßnahmen zur Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können?	❑
Bestehen Maßnahmen zur Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden?	❑
Bestehen Maßnahmen zur Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können?	❑
Bestehen Maßnahmen zur Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können?	❑
Bestehen Maßnahmen zur Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind?	❑
Bestehen Maßnahmen zur Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können?	❑
Besteht eine Zertifizierung des Dienstleisters nach ISO 27001 oder ist etwas Vergleichbares vorhanden?	❑
Nach welchem Standard wurde der Schutz der Anwendung ausgerichtet?	❑
Werden Penetrationstests regelmäßig (alle 12 - 36 Monate) wiederholt?	❑
Welche organisatorischen Maßnahmen trifft der Dienstleister zum Schutz der Informationen/Daten (vgl. Abschnitt 8)?	❑

6. Aufnahme in das Verzeichnis der Verarbeitungstätigkeiten

Die DSGVO verpflichtet den Verantwortlichen für jede Verarbeitung gesondert zum Führen eines Verzeichnisses. Mithin muss auch das in diesem Rahmen entwickelte Verfahren nach den Anforderungen des Art. 30 DSGVO in das Verzeichnis aufgenommen werden.

Dieses muss enthalten:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
- die Zwecke der Verarbeitung
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

7. Durchführung einer Datenschutz-Folgenabschätzung

Die DSGVO definiert den Begriff der Datenschutz-Folgenabschätzung nicht. Sie kann als ein Instrument verstanden werden, das das - durch die Verarbeitung personenbezogener Daten verursachte - Risiko für die Rechte und Interessen der betroffenen Personen erkennt und bewertet.

Es handelt sich nicht nur um eine Risikomanagementaufgabe, sondern eine Risikominimierungsverpflichtung.

Gegenstand der Datenschutz-Folgenabschätzung ist nach dem Wortlaut des Art. 35 Abs. 1 Satz 1 DSGVO eine „Form der Verarbeitung" bzw. eine oder mehrere „Verarbeitungsvorgänge". Der Gesetzgeber verwendet weder den Begriff der „Verarbeitung", die in Art. 4 Nr. 2 DSGVO legaldefiniert ist, noch denjenigen der Verarbeitungstätigkeit aus Art. 30 Abs. 1 DSGVO. Er stellt also eher auf einzelne Vorgänge bzw. Formen innerhalb einer Verarbeitungstätigkeit ab.

Als einzelne Vorgänge kommen dabei das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten in Betracht (Art. 4 Nr. 2 DSGVO). Es kommen aber auch bestimmte Technologien oder spezielle Hard- oder Software in Frage.

In der Datenschutz-Folgenabschätzung zur virtuellen Jahreshauptversammlung wäre in einem ersten Schritt zu ermitteln, ob überhaupt eine Datenschutz-Folgenabschätzung erforderlich ist. Hierzu sind in jedem Fall die geplanten Verarbeitungsvorgänge und deren Zwecke zu ermitteln.

Aufgrund der Sensibilität und des Umfangs der hierbei verarbeiteten Daten und den möglichen finanziell schädlichen Folgen für die Teilnehmer ist die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung wahrscheinlich.

Achtung! Die finale Entscheidung, eine Datenschutz-Folgenabschätzung durchzuführen liegt bei jedem Unternehmen selbst.

Die DSGVO gestattet es auch nicht, eine zentrale, für alle genossenschaftlichen Unternehmen geltende Datenschutz-Folgenabschätzung durchzuführen. Datenschutz-Folgenabschätzungen sind von jedem Verantwortlichen selbst, unter Betrachtung der für ihn, etwa auch aus geographischer Sicht, relevanten Risiken, durchzuführen und jährlich neu zu bewerten.

Ferner ist auch die Frage der Anonymität, also der geheimen Wahl ein Thema, das auf seine Risiken hin bewertet werden sollte. Zudem muss eine Bewertung des Verfahrens unter Bezugnahme der einzusetzenden Technologie erfolgen.

Die Bewertungsphase ist elementarer Bestandteil jeder Datenschutz-Folgenabschätzung. Sie beinhaltet zunächst eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck. Bestandteil jeder Datenschutz-Folgenabschätzung ist damit eine Prüfung, ob bei der Verarbeitung der Grundsatz der Datenminimierung beachtet wird.

Soll die Verarbeitung aufgrund „berechtigter Interessen" des Verantwortlichen erfolgen, bedarf es im Rahmen der Verhältnismäßigkeitsprüfung auch einer Bewertung, ob die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person gegenüber den im Rahmen der systematischen Beschreibung dargelegten berechtigten Interessen überwiegen.

Das Bundesamt für Sicherheit in der Informationstechnik rechnet mit nachfolgenden Gefährdungen bei der Nutzung von Videokonferenzsystemen:

- Abhören von Videokonferenzen
- Manipulation der Signalisierung
- Ungeschützte oder unkontrollierte Verschlüsselungsendpunkte
- Unzureichend abgesicherte Cloud-Dienste
- Qualitätseinbußen durch unzureichende Dimensionierung
- Fehlerhafte Bedienung und Nutzung
- Automatische Annahme von eingehenden Verbindungsanfragen
- Gezieltes Ausspähen von Räumen
- Verlust der Vertraulichkeit durch Kompromittierung von Video-Endpunkten
- Leistungsüberwachung und Profiling
- Kein ordnungsgemäßer Benutzerwechsel für Video-Endpunkte
- Versehentliche Preisgabe von Informationen
- Unzureichende Prüfung der Identität von Kommunikationspartnern
- Fehlverhalten und Missbrauch von Sprachsteuerung und KI-Funktionen
- Übergreifende Wirkung eines Sicherheitsvorfalls
- Konfigurationsfehler bei Videokonferenzlösungen
- Missbrauch von Administrations- und Wartungszugängen
- Unzureichende Organisation des Betriebs eines Videokonferenzsystems
- Unzureichendes Identitäts- und Berechtigungskonzept
- Unzureichend abgesicherte Aufzeichnung, Protokollierung und Dateiablage
- Unzureichende Kenntnis von Technik und Regelungen.

8. Technische & organisatorische Maßnahmen

Die DSGVO verlangt auch vom Verantwortlichen die Umsetzung bzw. Kontrolle ausgelagerter geeigneter technischer und organisatorischer Maßnahmen. Vom Begriff der Maßnahme werden alle Handlungen erfasst, die in geeigneter Weise dem Ziel dienen, das auferlegte Ergebnis einer Datenschutzkonformität zu erzielen. Dies bedeutet, dass der Verantwortliche das Ziel der datenschutzrechtlichen Rechtmäßigkeit seines Handelns anstreben und für sein Erreichen einstehen muss. Hier gilt es, die in Abschnitt 2 benannten Datenschutzziele zu erfüllen. Diese sind entsprechend Art. 5 Abs. 2 DSGVO zu dokumentieren.

Hierzu können beispielhaft Maßnahmen in den nachfolgenden Bereichen gehören:

- Hinweise auf Videokameras, Einsehbarkeit aller Personen im Raum
- Verschlüsselung
- Verständnis der eingesetzten Anwendung
- Vier-Augen-Prinzip
- Hinweise auf nicht versenden von Nachrichten
- Positionierung von Cloud Connector und Video Edge Server in einer DMZ
- Bereitstellung von Informationen zur sicheren Nutzung von Videokonferenzen
- Deaktivierung der automatischen Annahme eines Video-Anrufs
- Absicherung von frei zugänglichen Video-Endpunkten
- Absicherung und Einschränkung von Auswertungen von Videokonferenzinhalten
- Beenden von Sitzungen und An-/Abmeldungen an Video-Endpunkten
- Absicherung von Konferenzräumen
- Unterschiedliche Profile für Videokonferenzen
- Sichere Konfiguration von geplanten Videokonferenzen
- Planung und Beschaffung der Videokonferenzlösung
- Erstellung eines Rollen- und Berechtigungskonzepts
- Sicherer Umgang mit Konferenzaufzeichnungen
- Erstellung von Fein- und Betriebskonzept für die Videokonferenzlösung
- Schulungen zur sicheren Nutzung von Videokonferenzen
- Penetrationstest der Videokonferenzlösung.

9. Kontinuierliche Überwachung

Letzten Endes gilt es, die Risikoeinschätzungen sowie die getroffenen Maßnahmen einer regelmäßigen, jährlichen, Kontrolle zu unterziehen.

Fazit

Die derzeitige Krise eröffnet insbesondere mit Blick auf virtuelle Jahreshauptversammlungen viele neue Möglichkeiten, aber auch neue rechtliche Herausforderungen. Gerade im Datenschutz sind viele Maßnahmen zum Schutz der Betroffenen zu treffen.

Das Auslassen dieser Themen kann schnell zu hohen Geldbußen in Höhe von bis zu 20 Millionen Euro führen. Zudem muss die Gültigkeit einer datenschutzrechtlich rechtswidrigen Abstimmung im Rahmen einer Jahreshauptversammlung in Frage gestellt werden.

Daher empfehlen wir, das Thema der virtuellen Jahreshauptversammlung mit der nötigen Aufmerksamkeit zu verfolgen und geeignete Maßnahmen zum Schutz der personenbezogenen Daten zu ergreifen.

.

Quellen/Literatur

- https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/2020/1-quartal/corona-gesetzespaket-im-bundesrat.html.
- BSI Kompendium Videokonferenzsysteme, KoViKo - Version 1.0.1
- Roßnagel, in Roßnagel, Das neue DSR, § 3 Rn. 42.
- Roßnagel, in Simitis/Hornung/Spiecker, Datenschutzrecht, Art 5, Rn. 21.
- Spoerr, in BeckOK DatenschutzR; DS-GVO Art. 28 Rn. 35; Kühling, in Buchner/Hartung, DS-GVO Art. 28 Rn. 60; Paal, in Pauly/Martini, DS-GVO Art. 28 Rn. 21; Eckhardt, CCZ 2017, 111 (114).
- Eckhardt, CCZ 2017, 111 (114).
- Moritz/Karg, in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 35 Rn. 9.
- Reibach, in Taeger/Gabel, DSGVO BDSG, Art. 35, Rn. 4.
- WP 248 Rev. 01, S. 8.
- Kurzpapier Nr. 5 der Datenschutzkonferenz vom 24.7.2017, S. 1.
- Laue, in Spindler/Schuster, Recht der elektronischen Medien, Art 35. Rn. 26.

KONTAKT

Ihr Datenschutzbeauftragter
E-Mail datenschutz@dz-cp.de
www.dz-cp.de

Zuständige Landesdatenschutzbehörde
Die Kontaktdaten der Datenschutzbeauftragten in den Bundesländern finden Sie unter anderem auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter:
www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

IMPRESSUM

Leitfaden Datenschutz in einer virtuellen Jahreshauptversammlung · Herausgeber: DZ CompliancePartner GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3324, Telefax 069 6978-3322, www.dz-cp.de, Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-Id-Nr.: DE201150917, Geschäftsführung: Jens Saenger (Sprecher), Andreas Marbeiter, Norbert Schäfer · Bildnachweise: © iStockphoto, Rawpixel ·