Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Friedrichstr. 219
10969 Berlin
Besuchereingang:
Puttkamer Str. 16-18

Telefon: (030) 13889-0
Telefax: (030) 215 50 50
mailbox@datenschutz-berlin.de

Sprechzeiten

tgl. 10-15 Uhr, Do. 10-18 Uhr
(oder nach Vereinbarung)

Erreichbarkeit

U6: Kochstr.
Bus: M29, 248

Internet

https://datenschutz-berlin.de

Empfehlungen für die Prüfung von Auftragsverarbeitungsverträgen von Anbietern von Videokonferenz-Diensten

In unserer aufsichtsbehördlichen Tätigkeit mussten wir feststellen, dass bestimmte Mängel in Auftragsverarbeitungsverträgen von Anbietern von Videokonferenz-Diensten häufiger auftauchen. Daher empfehlen wir den unserer Aufsicht unterliegenden Verantwortlichen, bei der Prüfung der Verträge insbesondere auf folgende Aspekte zu achten:

Wird der Dienstleistungsvertrag online abgeschlossen, ist sicherzustellen, dass der Auftragsverarbeitungsvertrag tatsächlich in den Vertrag einbezogen wird. Der Auftragsverarbeitungsvertrag muss alle Anforderungen des Art. 28 DS-GVO abdecken.

Insbesondere müssen die Anbieter vollständig weisungsgebunden handeln, dürfen also die personenbezogenen Daten nicht zu eigenen Zwecken oder Zwecken Dritter verarbeiten (Art. 28 Abs. 3 lit. a DS-GVO) und müssen sie sofort nach Abschluss der Leistungserbringung nach Wahl der verantwortlichen Stelle herausgeben oder löschen (Art. 28 Abs. 3 lit. g DS-GVO). Die Anbieter müssen sich zudem verpflichten, alle Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung zu stellen und Überprüfungen – einschließlich Vor-Ort-Inspektionen – zu ermöglichen und dazu beizutragen (Art. 28 Abs. 3 lit. h DS-GVO). Die Verpflichtung zur Bereitstellung muss alle erforderlichen Informationen umfassen und darf nicht etwa auf bestimmte für den vollständigen Nachweis nicht ausreichende Dokumente beschränkt werden. Ebenso darf das Kontrollrecht nicht etwa auf die Anforderung von oder die Einsicht in Unterlagen beschränkt werden. In ganz besonderen Ausnahmefällen muss auch eine unangekündigte Vor-Ort-Kontrolle möglich sein. Jedenfalls für Überprüfungen, die wegen Verstößen der Anbieter gegen ihre Pflichten erforderlich werden, muss eine Kostentragungspflicht der Verantwortlichen ausgeschlossen sein, da sonst das Überprüfungsrecht faktisch entwertet würde.

Anbieter müssen sich vertraglich verpflichten, alle nach Art. 32 DS-GVO erforderlichen technisch-organisatorischen Maßnahmen umzusetzen. Verweist der Vertrag auf eine abschließende Liste bestimmter umzusetzender Maßnahmen, ist dies in aller Regel nicht ausreichend.

Subunternehmer dürfen nur mit Zustimmung der verantwortlichen Stelle eingeschaltet werden (Art. 28 Abs. 2 DS-GVO); im Fall einer allgemeinen Erlaubnis für Subunternehmer müssen die Anbieter die verantwortliche Stelle proaktiv und rechtzeitig über geplante Subunternehmer informieren. Die Verantwortlichen müssen ein echtes Recht zum Einspruch gegen Subunternehmer haben, sodass nicht etwa nur das Nutzungsrecht für den Dienst entfallen darf, während die Vergütungspflicht bestehen bleibt. Alle Kontrollrechte müssen im vollen Umfang auch gegenüber Subunternehmern gelten (Art. 28 Abs. 4 S. 1 DS-GVO).

Insbesondere bei Anbietern mit Sitz oder Verarbeitungsort außerhalb von EU und EWR ist genau auf die vertraglichen Formulierungen zu achten. Wenn der Vertrag – wie Art. 28 Abs. 3 lit. a und h DS-GVO – Ausnahmen von der Weisungsbindung vorsieht, müssen diese exakt die nach dem Gesetz zulässigen Grenzen einhalten. Diese Ausnahmen dürfen sich ausschließlich auf das Recht der EU und soweit einschlägig der Mitgliedstaaten beziehen, damit nicht unzulässig Art. 48 DS-GVO umgangen wird.

Verantwortliche müssen nach Art. 5 Abs. 2 DS-GVO jederzeit nachweisen können, dass sie die gesetzlichen Anforderungen einhalten. Dies erfordert zwingend, dass einerseits der Auftragsverarbeitungsvertrag klar formuliert ist und keine Zweifel daran möglich sind, dass alle gesetzlichen Anforderungen eingehalten werden. Jegliche Unklarheiten und widersprüchliche Regelungen sind zu vermeiden, auch wenn es an anderer Stelle Klauseln gibt, die bei Widersprüchen einer der Regelungen Geltungsvorrang einräumen (Vorrangklauseln). Andererseits müssen auch die zulässigen Subunternehmer jederzeit klar festgelegt sein, sodass der reine Verweis im Vertrag auf eine Liste auf einer Webseite oder eine nur pauschale Bezeichnung wie „verbundene Unternehmen“ oder eine Angabe ohne vollständigen Namen incl. Rechtsform und Anschrift nicht ausreicht.

Erfolgt die Datenverarbeitung in Drittländern, also außerhalb des Geltungsbereichs der DS-GVO, muss die Übermittlung durch geeignete Garantien gesichert sein, etwa durch Vereinbarung der von der EU-Kommission genehmigten Standardvertragsklauseln. Dabei ist insbesondere zu beachten, dass die Rechte und Pflichten aus den Standardvertragsklauseln nicht eingeschränkt werden dürfen, auch nicht in anderen Vertragsdokumenten, weil sonst der Datenexport unzulässig wird. Unzulässig sind Einschränkungen auch dann, wenn vertragliche Vorrangregelungen bestehen. Denn eine Vorrangregelung enthalten bereits die Standardvertragsklauseln selbst, sodass ohnehin jede Einschränkung zivilrechtlich unwirksam ist; dennoch können nur unveränderte Standardvertragsklauseln für den Datenexport herangezogen werden. Zulässig sind nur Ergänzungen, die ausschließlich zu Gunsten der betroffenen Personen und des Datenschutzniveaus wirken. Soll für Datenexporte in die USA auf das Privacy Shield abgestellt werden, müssen die Verantwortlichen überprüfen, ob die Selbstzertifizierung tatsächlich vorliegt und ob sie alle verarbeiteten Daten und Zwecke umfasst, insbesondere auch Personaldaten (HR data).

Standardvertragsklauseln und Privacy Shield sind derzeit Gegenstand eines Verfahrens vor dem Gerichtshof der Europäischen Union und könnten in der Folge als von Anfang an unwirksam verworfen werden. Dies spricht dafür, die Datenverarbeitung auf den Bereich von EU und EWR und andere von der EU-Kommission als datenschutzrechtlich vergleichbare Staaten zu beschränken.

Bei der Benennung der betroffenen Personen ist zu beachten, dass ggf. auch über Dritte gesprochen wird, sodass auch deren personenbezogene Daten verarbeitet werden.