Datenschutz im Homeoffice

Viele Fachkräfte arbeiten während der derzeitigen Kitaschließung von zu Hause aus. So wie in der Kindertageseinrichtung ist auch zuhause auf den Datenschutz zu achten. Die LAG Freie Kinderarbeit steht allen Teilnehmer*innen des LAG-Datenschutzservices als Datenschutzbeauftragter auch zu den Fragen rund um die Umgestaltung der Arbeitsplätze in der Corona Krise beratend zur Seite.

Grundsätzlich gilt: Alle notwendigen Datenschutzmaßnahmen nach EU-Datenschutz Grundverordnung (EU-DSGVO) beziehen sich immer nur auf die Verarbeitung von personenbezogene Daten. Während also die Bearbeitung der Portfolioordner oder die Überarbeitung der Anmeldeliste datenschutzrelevante Aufgaben sind, trifft dies auf die Arbeit an der Konzeption oder die Lektüre eines Fachartikels nicht zu.

Nutzung privater Endgeräte

Nur die vom Arbeitgeber bereitgestellte Hard- und Software kann auch vom Arbeitgeber auf datenschutzkonforme Einstellungen kontrolliert werden (Virenschutzsoftware, aktuelles Betriebssystem etc.). Deshalb stellen größere Arbeitgeber ihren Mitarbeiter*innen dienstliche Geräte zur Verfügung. Kleinere Träger können es sich aber in der Regel nicht leisten, alle Mitarbeiter*innen mit einem Laptop auszustatten. Zudem arbeiten auch viele ehrenamtliche Vorstände an privaten PCs oder Laptops. Bei der Nutzung von privaten Geräten sollte auf jeden Fall dafür gesorgt werden, dass auch auf diesen ein einheitlicher Standard an Virenschutzsoftware und die aktuellste Version des benutzten Betriebssystems installiert ist. Zudem sollte es getrennte, passwortgeschützte Zugänge auf den Endgeräten geben, falls diese von mehreren Personen im Haushalt genutzt werden.

Speichern von personenbezogenen Daten

Ein weiteres Thema von datenschutzrechtlicher Relevanz ist das Speichern von personenbezogenen Daten. Dies sollte nicht auf privaten Speichermedien wie lokalen Festplatten oder ungesicherten USB-Sticks erfolgen. Personenbezogene Daten sollte ausschließlich auf Servern oder sonstiger Hardware des Trägers gespeichert werden, etwa auf passwortgeschützten USB-Sticks, die an die Mitarbeiter*innen verteilt werden. Eine technisch aufwändigere Variante ist ein VPN-Zugang, über den von zuhause aus auf den Server des Trägers – falls es einen Server gibt – zugegriffen werden kann.

Ausdrucken

Das Ausdrucken von Dokumenten mit personenbezogenen Daten im Homeoffice sollte auf das minimal erforderliche Maß beschränkt werden. Ausgedruckte Dokumente sind unmittelbar nach Wegfall ihres Verwendungszwecks zu vernichten. Soweit die Mitarbeiter*innen im Homeoffice nicht über datenschutzkonforme Aktenvernichtungsgeräte verfügen, was vermutlich eher selten der Fall sein dürfte, sollten Ausdrucke mit personenbezogenen Daten bei nächst möglicher Gelegenheit zur Vernichtung mit in die Einrichtung gebracht werden. Das Wegwerfen von Ausdrucken mit personenbezogenen Daten in den heimischen Hausmüll empfiehlt sich nicht.

Vor Zugang von Dritten schützen

Im Homeoffice muss sichergestellt sein, dass ausschließlich die Mitarbeiter*in Zugang zu den personenbezogenen Daten aus der Einrichtung hat. Weder Familienangehörige, Mitbewohner*innen noch sonstige Personen dürfen Zugriff auf die zu schützenden Daten erhalten. Aus diesem Grund sollten

die Mitarbeiter*innen angehalten werden, nach Möglichkeit in einem Raum zu arbeiten, der für dritte Personen nicht uneingeschränkt frei zugänglich ist. Wenn Mitarbeiter*innen an Dokumenten mit personenbezogenen Daten arbeiten, sollte der Bildschirm außerdem so positioniert sein, dass eine direkte Einsichtnahme durch Personen, die den Raum betreten, nicht möglich ist. Bei zeitweisem Verlassen des Zimmers, in dem die Homeoffice-Tätigkeit stattfindet, sollte der Laptop oder der PC ausgeschaltet oder zumindest eine passwortgesicherte Bildschirmsperre aktiviert werden. Aber nicht nur digitale, sondern auch analoge Dokumente, wie Portfolioordner, sind vor dem Zugriff von Dritten zu schützen und am besten in einem abschließbaren Schrank zu deponieren.

Kommunikationstechnologien

Ein weiteres großes Thema im Homeoffice ist die Nutzung von Kommunikationstechnologien. Da es sich bei Kommunikationstechnologien immer auch um potentielle Überwachungstechnologien handelt, ist hier größte Vorsicht angebracht. Das sieht auch der Gesetzgeber so: Die Einführung solcher Technologien ist nicht nur nach Datenschutzkriterien zu beurteilen, sondern auch mitbestimmungspflichtig nach dem Betriebsverfassungsgesetz – das heißt, wenn es einen Betriebsrat gibt, muss dieser in die Entscheidung für die Nutzung eines bestimmten Anbieters mit einbezogen werden. Wenn es keinen Betriebsrat gibt, ist dies nicht notwendig.

Die EU-DSGVO schreibt einen „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ vor (Art. 25 EU-DSGVO). Folgende Prüfungsmaßnahmen vor dem Einsatz von Video- und Onlinekonferenzanbietern empfiehlt etwa Rechtsanwalt Thomas Schwenke auf seiner Webseite datenchutz-generator.de:

- EU-Dienste vorziehen – Dienste aus anderen Ländern sollten ein gleichwertiges Datenschutzniveau nachweisen können.
- Dienste mit datenschutzfreundlichen Einstellungen wählen, das betrifft insbesondere folgende Themen:
    - **Verschlüsselung**: Übertragungen sollten verschlüsselt erfolgen.
    - **Geschäftsnutzung**: Die geschäftliche Nutzung sollte erlaubt sein (da datenschutzrechtliche Zusicherungen auf Geschäftskunden beschränkt sein können). Unter Umständen bieten auch nur bezahlte Versionen die erforderlichen Datenschutzfunktionen.
    - **Freigaben**: Bildschirmübertragung oder Aufzeichnung sollte eine ausdrückliche Zustimmung voraussetzen.
    - **Protokolle und Aufzeichnungen**: Gesprächsverläufe und Aufzeichnungen sollten grundsätzlich nach Gesprächsende gelöscht werden.
    - **Profiling**: Es sollten keine Verhaltensprofile der Teilnehmer gebildet werden oder diese Funktion sollte abgeschaltet werden können.

Auftragsverarbeitungsvertrag

Wenn die Entscheidung für einen Anbieter gefallen ist, muss mit diesem ein Auftragsverarbeitungsvertrag abgeschlossen werden, da es sich auch bei Video- oder Telefonkonferenzen um eine Auftragsdatenverarbeitung im Sinne der EU-DSGVO handelt. Bei kostenfreien Angeboten entspricht der Auftragsverarbeitungsvertrag den Datenschutzinformationen des Anbieters. Bei kostenpflichtigen Angeboten muss ein Vertrag abgeschlossen werden. Über folgende Punkte muss der Anbieter informieren:

- Darlegung der technischen und organisatorischen Maßnahmen zum Datenschutz des Anbieters sowie der datenschutzfreundlichen Voreinstellungen.
- Offenlegung, ob der Anbieter mit Subunternehmen zusammenarbeitet und wo Informationen über die Datenschutzmaßnahmen der Subunternehmen zu finden sind.

Da alle Kommunikationsteilnehmer*innen von Videokonferenzen (Mitarbeiter*innen, Netzwerkpartner*innen, Eltern etc.) informiert werden müssen, empfiehlt sich, diese Informationen in die reguläre Datenschutzerklärung des Trägers aufzunehmen. Auf die Datenschutzerklärung können Sie dann per Link zum Beispiel auf Login-Seiten oder in Einladungen zu einem Onlinemeeting hinweisen. Die Datenschutzerklärung kann mit Unterstützung von Datenschutzgeneratoren erstellt werden, beispielsweise mit dem datenschutz-generator.de.

Verzeichnis der Verarbeitungstätigkeiten

Jeder Träger ist verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen (Art. 30 DSGVO). Analog anderer Verarbeitungstätigkeiten, die alle im Verzeichnis der Verarbeitungstätigkeiten aufgeführt sind, müssen hier die gleichen Informationen zur Kommunikationstechnologie hinterlegt werden: Wer ist verantwortlich? Was ist der Zweck der Datenverarbeitung? Welche personenbezogenen Daten werden erhoben? Wie lange werden sie gespeichert? Durch welche technischen und organisatorischen Maßnahmen werden sie gesichert?