Homeoffice, aber sicher!

Regeln für das Homeoffice

Datenschutzfreundliche Anwendungen gewährleisten noch kein sicheres Homeoffice. Vielmehr sind einfache, aber wirkungsvolle Regeln für die Einrichtung und das Verhalten bei der Arbeit zu Hause zu beachten. Die Datenschutzbeauftragte publizierte einen Leitfaden, der kurz und bündig die wesentlichen Punkte zusammenfasst.

Die öffentliche Diskussion drehte sich um technische Voraussetzungen für die Zusammenarbeit auf Distanz. Diese waren grundlegend für das Funktionieren der Verwaltung und anderer Institutionen im ersten Jahr der Corona-Pandemie. Doch blieben die Risiken kaum beachtet, die damit verbunden waren, dass plötzlich Personendaten und heikle Geschäftsdaten nicht mehr im gesicherten Umfeld des Büros, sondern im Wohnzimmer bearbeitet wurden. Der private Computer diente zum Beispiel nicht mehr nur dem Gamen, sondern es wurden darauf beispielsweise die Personendaten von Sozialhilfeempfängerinnen und Sozialhilfeempfängern bearbeitet. Da die Schulen geschlossen waren, hielten sich auch Kinder in der Nähe des behelfsmässig eingerichteten Arbeitsplatzes am Esstisch auf und hörten bei der Videokonferenz mit.

Die Herausforderung fängt also mit dem richtigen Arbeitsplatz innerhalb der eigenen vier Wände an. Wo kann ungehindert am Bildschirm gearbeitet werden, ohne dass Dritte Einblick in die Informationen bekommen? Wie kann ungestört und ohne Zuhörende aus dem Familienumfeld telefoniert werden? Auch im digitalen Zeitalter bestehen analoge Probleme: Wie können Papiere verwahrt und ungehindert bearbeitet werden, ohne Informationen offenzulegen? Was kann in der Altpapiersammlung entsorgt werden? Diese wenigen Fragen zeigen, was alles zu beachten ist.

Einfache Massnahmen können ein gutes Mindestmass an Sicherheit gewährleisten. Jedoch muss das Bewusstsein für die Risiken vorhanden sein. Der Schwatz bei der Kaffeemaschine im Büro ist weit weniger verfänglich, als ein Gespräch mit dem Partner oder der Partnerin beim Teekochen in der privaten Wohnung. Das Homeoffice verlangt nach kleinen Verhaltensanpassungen aller Mitarbeitenden, die zur täglichen Routine werden müssen.

Die Datenschutzbeauftragte beleuchtet im Leitfaden 8 Regeln für das Homeoffice auch die technischen Aspekte, die den Datenschutz im Homeoffice gewährleisten. Wenn mit privaten Geräten gearbeitet wird oder Geräte im Einsatz sind, die nicht zentral über die Informatikabteilung gewartet werden, ist die Eigenverantwortung besonders wichtig. Auch im klassischen Büroumfeld gelingen Angriffe auf die Informationssicherheit meist über die Mitarbeitenden – Stichwort Social Engineering. Wenn in privaten Räumlichkeiten gearbeitet wird, nimmt dieses Risiko stark zu. Im Homeoffice bestehen zusätzliche Ablenkungsfaktoren. Ein Mausklick, der zu schnell oder zu viel gemacht wird, kann zu grösserem Schaden führen, auch weil sich private und geschäftliche Informationen auf dem benutzten Gerät vermischen. Bei der Arbeit zu Hause sind deshalb Routinen strikt einzuhalten, E-Mails von unbekannten Absendern besonders zu prüfen sowie System- und Softwareaktualisierungen regelmässig zu installieren.

8 Regeln für das Homeoffice auf
www.datenschutz.ch

Komplexe Fragen zur digitalen Zusammenarbeit

Aussergewöhnliche Zeiten verlangen nach aussergewöhnlichen Massnahmen. Dennoch dürfen sicherheitsrelevante Aspekte nicht vernachlässigt werden. Die neue Situation im Homeoffice verunsicherte die Mitarbeitenden öffentlicher Organe. Die Datenschutzbeauftragte publizierte deshalb zu Beginn des ersten Lockdowns eine Produkteliste für die digitale Zusammenarbeit.

Öffentliche Organe tragen eine besondere Verantwortung für die Personendaten der Einwohnerinnen und Einwohner. Datenschutz funktioniert präventiv. Wenn Personendaten in die falschen Hände geraten sind, kann die Kontrolle darüber nicht mehr zurückerlangt werden.

Soforthilfe geleistet

Homeoffice und Homeschooling kamen plötzlich. Das weitere Funktionieren der Verwaltung und des Schulbetriebs war nur dank digitaler Produkte möglich. Schnelles Handeln war auch für die Datenschutzbeauftragte angesagt. Sie prüfte die am meisten angefragten Produkte zur digitalen Zusammenarbeit summarisch und veröffentlichte innert wenigen Tagen eine Produkteliste auf ihrer Website. In- und ausländische Datenschutzstellen, aber auch Bildungsdirektionen und Bildungsministerien verwiesen während des Lockdowns auf die Zürcher Datenschutzwebsite.

Die Entscheidung für ein bestimmtes Produkt liegt beim öffentlichen Organ. Es bleibt für die Personendaten verantwortlich und darf auch unter Druck die Sicherheit der Personendaten nicht vernachlässigen. Nicht jedes Produkt ist für jeden Zweck geeignet. Das öffentliche Organ muss in jedem einzelnen Fall überlegen, zu welchem Zweck ein digitales Produkt genutzt werden soll. Für die Auswahl eines Produkts spielt die Art der bearbeiteten Personendaten ebenso eine Rolle wie die Geschäftsbedingungen des Anbieters. Das öffentliche Organ muss wissen, welches Recht angewendet wird, welcher Gerichtsstand gilt, ob ein Kontrollrecht verankert ist, wo die Daten bearbeitet und welche Cookies eingesetzt werden. Die Möglichkeiten der Datenverschlüsselung sind von zentraler Bedeutung. Die Anforderungen stehen im Leitfaden der Datenschutzbeauftragten Bearbeiten im Auftrag konkretisiert. In einer umfassenden Analyse sind die Risiken im Einzelfall abzuwägen mit Blick auf die vom Gesetz geforderten Massnahmen und von den Anbietern erfüllten Anforderungen.

Risikoanalyse vor dem Einsatz
Datenschutzkonforme oder zumindest datenschutzfreundliche Messengers und Videokonferenzsysteme auszuwählen, ist schwierig. Die Plattformen verfügen über unterschiedliche Funktionen von der reinen Kommunikation über das Teilen von Dokumenten bis zum Speichern des Gesprächsinhalts. Aber allen Produkten ist gemeinsam, dass sie die Anforderungen einer Auslagerung respektive einer Auftragsdatenbearbeitung erfüllen müssen. Beim Anbieter einer Kommunikationsplattform fallen zudem viele Randdaten wie Name, IP-Adresse oder Dauer des Gesprächs an. Diese werden in einer Cloud gespeichert und in vielen Fällen bis zum Löschen des Kontos aufbewahrt.

Die Datenschutzbeauftragte prüfte Messengers und Videokonferenzsysteme anhand der Dokumente, welche die Anbieter zur Verfügung stellten. Sie veröffentlichte ein Merkblatt Messengers und Videokonferenzsysteme mit einer Beurteilung nach den wichtigsten Kriterien.

Vor dem Einsatz eines Produkts muss das öffentliche Organ entscheiden, welches Produkt für die jeweilige Kommunikation geeignet ist. Für sensitive Bereiche wie die Strafverfolgung oder im Spitalbereich können gewisse Produkte ungeeignet sein. Der konkrete Sachverhalt ist auch hier zu berücksichtigen. Ein Produkt kann in einem Spital vielleicht intern zum Austausch im administrativen Bereich genutzt werden, ist aber ungeeignet für die Nutzung in Bereichen, in denen auch Patientendaten übermittelt werden. Das Merkblatt Messengers und Videokonferenzsysteme unterstützt bei dieser Risikoabwägung mit Fragen und Tipps:

- Zu welchem Zweck soll die Software eingesetzt werden?
- Welche Arten von Informationen sollen ausgetauscht werden?
- In welchem Bereich soll die Software eingesetzt werden?
- Welches Recht ist anwendbar und welcher Gerichtsstand gilt?
- Wo werden die Randdaten gespeichert: im EU-Raum, in der Schweiz oder in anderen Ländern?
- Gibt es eine Verschlüsselung?
- Gibt es eine Zwei-Faktor-Authentifizierung?

Nach der Auswahl einer Anwendung muss entschieden werden, welche weiteren Massnahmen je nach Nutzung umgesetzt werden sollen. So kann das Speichern von Dokumenten und Gesprächsinhalten gesperrt oder das Attention Tracking deaktiviert werden.

Microsoft 365 in der Verwaltung
Organe der Verwaltung möchten Microsoft 365 datenschutzkonform nutzen. Sie drängen auf eine Antwort der Datenschutzbeauftragten. Die Konferenz der schweizerischen Datenschutzbeauftragten privatim unterstützte die Schweizerische Informatikkonferenz (SIK) bei Verhandlungen mit Microsoft. Daraus entstand der SIK-Rahmenvertrag, in dem für Datenschutzbelange die Anwendung von schweizerischem Recht und ein schweizerischer Gerichtsstand verankert sind. Trotzdem muss auch bei dieser Auslagerung eine Risikoabwägung vorgenommen werden. Es gilt zu beurteilen, mit welchen Produkten des Microsoft-365-Pakets welche Personendaten ausgelagert werden sollen. Neben dem Ort der Speicherung sind die Zugriffsberechtigungen und die Art der Verschlüsselung zu berücksichtigen. Zusätzlich sind ausländische Gesetze wie der CLOUD Act zu beachten. In diesem Zusammenhang sind Personendaten unter speziellen Geheimnispflichten wie dem Berufs- oder Steuergeheimnis im Rahmen der Risikoanalyse besonders zu berücksichtigen.

Schrems II oder der ungenügende Schutz durch das Privacy Shield
Im letzten Sommer stufte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte die USA als Land mit nicht angemessenem Datenschutzniveau ein. Er reagierte damit auf ein Urteil des Europäischen Gerichtshofs, in dem der Datenschutz durch das Privacy-Shield-Abkommen als ungenügend eingeschätzt wird (Schrems II). Auch die Standardvertragsklauseln sind allein nicht ausreichend für einen Transfer von Personendaten in Länder ohne angemessenen Datenschutz. Deshalb müssen neue Wege gesucht werden, um die Personendaten angemessen zu schützen. Verschiedene Stellen erarbeiten Lösungsansätze. Auf europäischer Ebene werden die Standardvertragsklauseln revidiert.

Nutzen öffentliche Organe Cloud-Dienste, die einen Transfer von Personendaten in die USA beinhalten, müssen sie mit einer Kombination von rechtlichen und organisatorisch-technischen Massnahmen einen angemessenen Schutz sicherstellen. Eine hybride Cloud, bei der ein Teil der Personendaten lokal gespeichert wird, oder zusätzliche vertragliche Absicherungen vermindern beispielsweise das Risiko. Weitere Möglichkeiten sind etwa Verschlüsselung der Personendaten, wenn der Schlüssel beim öffentlichen Organ liegt, oder die Pseudonymisierung der Personendaten.

Die Datenschutzbeauftragte informiert auf ihrer Website www.datenschutz.ch über die Entwicklungen in diesem Bereich.

Prorektor-Wahl per Videokonferenz

Informationen in Bewerbungsdossiers stellen Persönlichkeitsprofile und somit besondere Personendaten dar. Sie bedürfen eines besonderen Schutzes bei der Bearbeitung. Die Datenschutzbeauftragte beantwortete die Frage, ob die Wahl des Prorektors einer Berufsschule als Videokonferenz durchgeführt werden darf.

In der Praxis werden dem Gesamtkonvent alle Bewerbungsunterlagen vorgestellt. Die Datenschutzbeauftragte hat dies als unverhältnismässig beurteilt. Zwar wird bei den Bewerbenden eine Einwilligung eingeholt. Diese kommt jedoch nicht freiwillig zustande, da sie für die Teilnahme am Bewerbungsverfahren vorausgesetzt wird. Bei der digitalen Durchführung des Verfahrens bestehen zusätzliche Risiken für die Persönlichkeitsrechte, da die Bewerbungsunterlagen hier einfacher weiterverbreitet werden können. Die Verhältnismässigkeit, aber auch die Informationssicherheit sind deshalb noch stärker zu berücksichtigen. Die Aufnahmefunktion des Videokonferenztools ist zu deaktivieren und den Teilnehmenden ist die Aufnahme mit Hinweis auf die Strafbarkeit zu untersagen. Die Wahl selber ist entweder brieflich oder mit verschlüsselten E-Mails durchzuführen, damit das Wahlgeheimnis gewährleistet ist.

Corona-Pandemie und Privatsphäre – als Video

Die Öffentlichkeit diskutierte im letzten Jahr ausgiebig über Privatsphäre und Datenschutz. Oft zeigte sich, dass die Grundsätze dieser Grundrechte wenig bekannt sind. Dies trifft nicht zu auf die Teilnehmenden des Datenschutz-Video-Wettbewerbs. Ihre Beiträge beschäftigen sich mit der Frage, wie viel Persönliches wir in Zeiten von Corona freiwillig und unfreiwillig preisgeben.

Die Zugangsweisen der jungen Videomaker und Youtuber sowie die Aspekte, die sie in ihren Videos behandeln, könnten nicht unterschiedlicher sein. Beim erstplatzierten Beitrag handelt es sich um eine kleine Tragikomödie. Sehr prägnant illustriert der Kurzfilm die Tücken des Homeoffice: In einem Videocall offenbart ein geschätzter Mitarbeiter Einblicke in sein Privatleben, die seinen Chef quasi gegen den eigenen Willen dazu bringen, ihn zu entlassen. Die weiteren ausgezeichneten Videos befassen sich mit der allgemeinen Unsicherheit in der bedrohlichen Krisensituation. Der zweitplatzierte Beitrag nutzt dafür eine witzige Animation, während das drittplatzierte Video auf schnelle und direkte Tiktok-Ästhetik setzt. Wie viele persönliche Informationen muss ich zur Eindämmung der Virusverbreitung bekanntgeben? Und bin ich sicher, dass meine Solidarität nicht missbraucht wird?