Outsourcing und Cloud Computing

Cloud Computing im Trend

Die Auslagerung von Datenbearbeitungen in die Cloud bringt grundlegende Veränderungen mit sich. Daten lassen sich dadurch schnell, einfach, vielfältig, ortsunabhängig und zu niedrigen Kosten bearbeiten – der Attraktivität dieser Attribute können sich weder die Verwaltung noch die Privaten entziehen. Doch die Aspekte des Datenschutzes und der Informationssicherheit dürfen nicht in den Hintergrund treten.

Mangelnde Transparenz und Kontrollverlust

Im Gegensatz zu einer klassischen Auslagerung sind Cloud-Dienste standardisiert und die Nutzungs- und Vertragsbedingungen meistens vom Anbieter vorgegeben. Sie sind oft nicht datenschutzkonform. Das öffentliche Organ bleibt auch bei der Inanspruchnahme von Cloud-Diensten für die Datenbearbeitung verantwortlich, sieht sich aber mit neuen Risiken konfrontiert. So ist oft nicht bekannt, wo die Daten gespeichert werden und wer die Subauftragnehmer sind. Der Einfluss des Auftraggebers auf die Sicherheitsmassnahmen sinkt. Die neuen Risiken können unter den Begriffen unzureichende Transparenz und Kontrollverlust zusammengefasst werden.

Mit der Risikoanalyse anfangen

Bevor ein öffentliches Organ einen Cloud-Dienst einsetzt, muss es als Erstes klären, ob die Daten überhaupt ausgelagert werden dürfen. Wenn Geheimnispflichten dem entgegenstehen, kann allenfalls eine Verschlüsselung verhindern, dass Dritte Kenntnis von den Daten nehmen können. Weiter ist durch eine Risikoanalyse zu prüfen, ob die Sensitivität der Daten mit den Risiken einer Auslagerung in die Cloud zu vereinbaren ist. Kriterien sind beispielsweise das Datenschutzniveau des Landes, in dem die Daten gespeichert werden, oder die eingesetzte Technologie. Aufgrund des Resultats der Risikoanalyse müssen die Informationssicherheitsmassnahmen definiert werden. Erst jetzt kann die Auswahl eines Anbieters beginnen, mit dem ein datenschutzkonformer Vertrag ausgearbeitet wird.

Pflichten bleiben trotz Vertrag erhalten

Allein der Abschluss eines datenschutzkonformen Vertrags entbindet das öffentliche Organ nicht von weiteren Pflichten. Je nach Cloud-Dienst sind bei der konkreten Nutzung weitere organisatorische und technische Massnahmen zu berücksichtigen.

Schutz des Berufsgeheimnisses in der Cloud

Der Datenschutzbeauftragte wurde mehrfach angefragt, ob und wie Produkte zur Datenbearbeitung im Gesundheits-, Schul- oder Verwaltungsbereich eingesetzt werden können, die nur unter Nutzung einer Cloud funktionieren. Er hat abgeklärt, unter welchen Voraussetzungen das Berufsgeheimnis eine Auslagerung in die Cloud zulässt.

Cloud-Anbieter darf keine Kenntnis erlangen

Ein Gutachten von Dr. Wolfgang Wohlers, Professor für Strafrecht und Strafprozessrecht an der Universität Basel, befasst sich mit der Rechtslage einer Auslagerung unter Beachtung des Berufsgeheimnisses nach Art. 321 StGB. Wohlers kommt zum Schluss, dass Datenbearbeitungen, die dem Berufsgeheimnis unterliegen, nur in die Cloud ausgelagert werden können, wenn der Cloud-Anbieter von den Daten keine Kenntnis erlangen kann.

Verschlüsselung und vertragliche Absicherung

Der Bearbeitung im Auftrag dürfen grundsätzlich keine Geheimnispflichten entgegenstehen. Deshalb müssen die Daten verschlüsselt werden, um die Kenntnisnahme der Informationen durch Dritte zu verhindern. Gemäss Gutachten muss der Schlüssel beim Auftragnehmer verbleiben. Eine weitere Möglichkeit sieht der Datenschutzbeauftragte in der vertraglichen Absicherung. Der Auftragnehmer verpflichtet sich damit, den Schlüssel nur auf ausdrückliche Anfrage und nach ausdrücklicher Einwilligung des Auftraggebers einzusetzen und auf die Daten zuzugreifen. Ein Zugriff auf die Daten muss im Einzelfall auch möglich sein, wenn dies für die sachgerechte Erledigung des Auftrags notwendig und für den Geheimnisherrn vorhersehbar ist, etwa bei der Wartung medizinischer Geräte. Zudem kann immer ausgelagert werden, wenn die betroffene Person einwilligt. Das öffentliche Organ muss in jedem Fall alle zum Schutz der Daten notwendigen Sicherheitsmassnahmen umsetzen.

Dropbox & Co. in den Schulen

Cloud-Dienste sind aus dem Schulalltag nicht mehr wegzudenken. Der Datenschutzbeauftragte beschäftigt sich in der Beratungspraxis ständig mit Produkten wie Google Drive, Office 365, Apple School Manager, Lehrer Office und Dropbox.

Schulen bleiben für ihre Daten verantwortlich

Bei Cloud-Diensten ist auch im Schulbereich die sorgfältige Abklärung der datenschutzrechtlichen Aspekte zwingend. Nicht alles, was möglich ist, ist erlaubt. Die Nutzung von Cloud-Diensten ist eine Auslagerung der Datenbearbeitung. Die Schule bleibt auch in diesem Fall für ihre Daten verantwortlich.

Fragen zum Schutz der Privatsphäre und zur Sicherheit der Daten müssen vor dem Einsatz solcher Produkte geklärt werden. Die Schulverantwortlichen müssen sich überlegen, wie ein Produkt zu welchen Zwecken und mit welchen Daten genutzt werden soll. Sie müssen die Verantwortlichkeiten bestimmen und Zugriffe, E-Mail-Adressen, Authentifizierungsmechanismen und vieles mehr festlegen. Die Daten müssen klassifiziert und die Lehrpersonen sowie Schülerinnen und Schüler über eine korrekte Nutzung instruiert werden. Bei jüngeren Schülerinnen und Schülern müssen die Schulen die Eltern informieren, wenn im Internet personenbezogene Rückschlüsse möglich sind, weil beispielsweise die E-Mail-Adressen den vollständigen Namen des Kindes mit der Schule verbinden oder wenn sie auch zu Hause den Cloud-Dienst benutzen sollen.

Unterstützung bei den Verträgen

Schulen verfügen oft nicht über Expertenwissen zu den rechtlichen Aspekten einer Vertragsschliessung, weshalb sie sich an den Datenschutzbeauftragten wenden können. Für die Nutzung von Office 365 konnte mit dem Hersteller Microsoft eine datenschutzkonforme Lösung vereinbart werden. Dafür hat Educa.ch für die Volksschulen und Switch für die Hochschulen einen Rahmenvertrag mit dem Hersteller abgeschlossen. Die Schulen müssen die Beitrittserklärung zu diesem Vertragswerk ausfüllen und die erwähnten Massnahmen zum Schutz der Daten definieren und umsetzen.

«Die Risiken des Cloud Computing können unter den Begriffen unzureichende Transparenz und Kontrollverlust zusammengefasst werden.»

Cloud Computing in der Verwaltung

Der Datenschutzbeauftragte prüft vermehrt Verträge von Behörden, Spitälern und anderen öffentlichen Organen mit Cloud-Anbietern. Die Anfragen reichen von der Speicherung und Bearbeitung von Daten in einem Traumaregister über die Inanspruchnahme von Amazon Web Services und den Einsatz von E-Recruiting Tools, Austauschplattformen oder einer Newsletter-Software bis hin zur kompletten Auslagerung der IT-Infrastruktur.

In allen Fällen sind die Anforderungen des IDG umzusetzen. Das öffentliche Organ muss die Dienste sorgfältig auf die datenschutzrechtlichen Anforderungen überprüfen. Der Leitfaden Bearbeiten im Auftrag des Datenschutzbeauftragten beinhaltet Checklisten und Übersichten für das Vorgehen, die Vertragsbestimmungen und die zu implementierenden Informationssicherheitsmassnahmen.

Sicherheitsmassnahmen definieren

Beim Cloud Computing müssen im Rahmen einer Risikoanalyse die Informationssicherheitsmassnahmen definiert werden, die zum Schutz der Daten notwendig sind. Unterliegen die Daten dem Berufsgeheimnis, müssen sie immer verschlüsselt werden und das Schlüsselmanagement muss beim öffentlichen Organ liegen. Ist dies nicht möglich, sind zusätzliche vertragliche Absicherungen notwendig. Auf jeden Fall sollte das Land, in das die Datenbearbeitungen ausgelagert werden, über ein angemessenes Datenschutzniveau verfügen.

Transparenz der Auftragnehmer

Umfassende Transparenz des Auftragnehmers über die Sicherheitsmassnahmen, die Kontrollmöglichkeiten, die Subauftragnehmer und die Orte der Datenbearbeitung helfen, eine datenschutzkonforme und sichere Lösung zu finden.

Bevölkerungsbefragung mit Online-Tool

Eine Gemeinde führte unter anderem über ein Online-Tool auf ihrer Website eine Bevölkerungsbefragung durch. Eine Privatperson meldete dem Datenschutzbeauftragten, dass bei der Online-Befragung die IP-Adressen gespeichert würden und somit die Anonymität der Umfrageteilnehmenden nicht gewährleistet sei.

Der Datenschutzbeauftragte wandte sich zur Abklärung des Sachverhalts an die Gemeinde. Es zeigte sich, dass sie einen Dritten mit der Bevölkerungsbefragung beauftragt hatte, der wiederum das Online-Tool eines US-amerikanischen Anbieters einsetzte.

Antworten und Adressen nicht getrennt

Da die Umfrage mit der freiwilligen Teilnahme an einer Verlosung verbunden war, umfassten die gespeicherten Daten unter anderem die IP-Adresse, die Umfrageantworten sowie die Adresse für die Wettbewerbsteilnahme. Die Daten wurden zusammen in einem Datensatz abgespeichert. Die Speicherung der IP-Adresse und der Einsatz eines sogenannten IP-Blockers sollten die Mehrfachteilnahme an der Umfrage verhindern.

Der Auftragnehmer der Gemeinde exportierte die Datensätze aus dem Online-Tool und löschte die IP-Adressen. Die Adressdaten für die Wettbewerbsteilnahme trennte er von den Umfrageantworten und speicherte sie randomisiert ab. Die restlichen Daten speicherte er gemeinsam.

Ungenügende Vertragsbedingungen des Online-Anbieters

Der Datenschutzbeauftragte prüfte die Durchführung der Online-Umfrage sowie das Auslagerungsverhältnis zwischen der Gemeinde beziehungsweise dem von ihr beauftragten Dritten und dem Online-Tool-Anbieter. Er kam zum Schluss, dass die Datenerhebung personenbezogen durchgeführt worden war. Die Anonymität der Umfrageteilnehmenden war nicht gewährleistet, weil die Daten in jeweils einem Datensatz gespeichert wurden. Zudem beurteilte er die Speicherung der IP-Adresse als unverhältnismässig. Der Einsatz des IP-Blockers war nicht geeignet, die Mehrfachteilnahme zu verhindern, da die Umfrage auch in Papierform und durch Befragen von Passantinnen und Passanten erfolgt war. Weiter waren die Vertragsbedingungen des Online-Tool-Anbieters in verschiedener Hinsicht ungenügend und somit die Auslagerung der Personendaten in die USA nicht datenschutzkonform. Daraus folgerte der Datenschutzbeauftragte, dass die Gemeinde ihre Verantwortung, die sie gegenüber den Umfrageteilnehmenden am Schutz ihrer Personendaten trägt, ungenügend wahrgenommen hatte.

§ 8 IDG
§§ 6 IDG i.V.m. 21 IDV