Cloud-Computing im Wirbel der kantonalen Datenschutzgesetze

Als Ende Juni 2021 bekannt wurde, dass der Bund Daten auf Clouds von amerikanischen und chinesischen Cloud-Providern auslagern wird, war der Aufschrei in der Bevölkerung gross. «Daten sollen besser von Schweizer Cloud-Providern in der Schweiz gespeichert werden», dachte sich wohl so mancher Bürger. Doch sind Daten in den Händen (ausländischer) Cloud-Provider wirklich ungenügend geschützt?

Von Nadine Rinderknecht

Diese Frage zielt zunächst auf faktische Sicherheit ab, was hier allerdings nicht analysiert werden kann. Vielmehr wird das geltende Recht in denjenigen Punkten beleuchtet, welche in Cloud-Konstellationen von besonderer Relevanz sind. Insofern können Antworten im Datenschutzrecht des Bundes bzw. in den Datenschutzrechten der Kantone – in diesem Beitrag mit Schwerpunkt auf dem Gesetzesrecht – gefunden werden. Letztere enthalten eine Vielzahl an unterschiedlichen Bestimmungen, welche im Grundsatz ähnlich zueinander sind, aber doch in einigen Punkten voneinander abweichen. Nach einer kurzen Einführung in die Cloud sowie in das Verhältnis zwischen dem Datenschutzrecht des Bundes und der Kantone vergleicht dieser Beitrag einige der kantonalen Bestimmungen im Hinblick auf den Auslandtransfer, die Informationssicherheit und die Datenschutzaudits.

Cloud-Dienstleistungen und Cloud-Computing

Wie das eingangs erläuterte Beispiel aufzeigt, nehmen öffentliche Organe zunehmend Cloud-Dienstleistungen in Anspruch. Dies sind Dienstleistungen, die dem Nutzer durch Cloud-Provider über das Internet bereitgestellt werden.

- Hierbei kann zwischen verschiedenen Haupttypen der Computing-Services differenziert werden: So kann ein Cloud-Provider dem Nutzer seine Infrastruktur (Infrastructure-as-a-Service), Plattform (Platforms-as-a-Service) oder Software (Software-as-a-Service) bereitstellen.

- Zudem bestehen verschiedene Formen der Bereitstellung: Gehören die Cloud-Umgebungen nicht dem Endnutzer, spricht man von sog. Public Clouds (z.B. Microsoft Azure, Google Cloud). Dahingegen sind die Cloud-Umgebungen von sog. Private Clouds nur einem Endbenutzer oder einer Gruppe von Endbenutzern zugeteilt (z.B. firmeneigene Rechenzentren). Weitere Haupttypen sind etwa die sog. Hybrid Clouds und sog. Multi-Clouds, die hier aber nicht näher erörtert werden.

Datenschutzrecht des Bundes und der Kantone

Werden Personendaten in eine Cloud geladen, modifiziert, gelöscht usw., kommt das Datenschutzrecht zur Anwendung. Es bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden (vgl. Art. 1 DSG). Erfolgt die Datenbearbeitung durch Bundesorgane oder private Personen, ist das Bundesrecht in der Form des DSG anwendbar (Art. 2 Abs. 1 DSG). Bearbeitet dahingegen ein kantonales Organ Personendaten, ist (mit wenigen Ausnahmen) das jeweilige kantonale Datenschutzrecht anwendbar (z.B. das Zürcherische IDG). Doch weil die 26 Kantone unterschiedliche Datenschutzgesetze haben, variieren die einzelnen Bestimmungen. Da sich diese aber oft nur in einigen Punkten unterscheiden (siehe auch die nachstehenden Ausführungen), besteht grundsätzlich für alle Kantone ein ähnlich hohes Schutzniveau. Letztens ist allgemein anzumerken, dass die Datenbearbeitung durch den Cloud-Anbieter eine Auftragsbearbeitung (Bearbeitung durch Dritte) darstellt, welche von den kantonalen Datenschutzgesetzen grds. zugelassen wird.

Auslandtransfer

Stehen die Server eines Cloud-Providers nicht in der Schweiz, geht mit der Auslagerung der Daten auch eine Datenübertragung in ein anderes Land einher. Dabei müssen die Bestimmungen zum Auslandtransfer eingehalten werden, welche oft zweigliedrig ausgestaltet sind: Zunächst fragt sich, ob das Zielland ein angemessenes Datenschutzniveau aufweist (z.B. § 14 Abs. 3 AG-IDAG). Ist dies nicht der Fall, kann eine grenzüberschreitende Bekanntgabe dennoch stattfinden, wenn eine bestimmte Voraussetzung wie ein überwiegendes Interesse oder ein Zusammenhang mit Rechtsansprüchen vor Gericht erfüllt ist (z.B. § 14 Abs. 4 AG-IDAG).

Hierbei unterscheiden sich die kantonalen Regelungen besonders hinsichtlich der Anzahl an möglichen Rechtsgrundlagen innerhalb des zweiten Schritts, indem weitere Grundlagen zu den soeben erwähnten hinzukommen: so eine hinreichende (vertragliche)

Garantie, Einwilligung der betroffenen Person, Zusammenhang mit einem Vertrag, Schutz der betroffenen Person, den Fall, dass die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat, sowie die Bekanntgabe bei bestimmten gesellschaftsrechtlichen Konstellationen (z.B. Art. 10a Abs. 2 GL-DSG). Hinzu kommt gemäss einigen wenigen Datenschutzgesetzen, dass die Übermittlung zu unterbleiben hat, wenn sie gegen die schweizerische Rechtsordnung oder die *ordre public* verstossen würde (z.B. Art. 11b Abs. 4 SH-DSG; § 10a Abs. 3 ZG-DSG).

Allerdings können die Bestimmungen auch nur eingliedrig ausgestaltet sein. Das massgebliche – und nach dem Wortlaut einzige – Kriterium besteht dann in einer allfälligen schwerwiegenden Gefährdung der Persönlichkeit der betroffenen Person (z.B. § 18 SZ-ÖDSG). Letztens verweisen einige kantonale Datenschutzgesetze bloss auf das DSG (z.B. Art. 27 Abs. 1 NE-CPDT), oder es fehlt gänzlich an einer Regelung zum Auslandtransfer (z.B. Graubünden, Obwalden).

Im Ergebnis sind grenzüberschreitende Bekanntgaben unter bestimmten Voraussetzungen zulässig. Allerdings kann die **Länge des Katalogs der zulässigen Rechtsgrundlagen erheblich variieren.** Insbesondere ist die Einwilligung der betroffenen Person nicht immer explizit im Katalog enthalten (z.B. § 14 Abs. 4 AG-IDAG).

Datensicherheit

Wurden Personendaten in eine Cloud geladen, müssen sie ihre Vertraulichkeit, Integrität und Verfügbarkeit durch bestimmte Vorkehrungen geschützt werden. Dabei unterscheiden sich die kantonalen Datenschutzgesetze oft nur im Konkretisierungsgrad ihres Wortlauts. Dies betrifft einerseits die vorzunehmende Handlung («angemessene Sicherung», § 13 Abs. 1 TG-DSG; «technische und organisatorische Vorkehrungen», Art. 16 Abs. 1 AR-DSG). Andererseits fällt auch die Nennung der Schutzziele teilweise sehr generell («unbefugtes Bearbeiten», Art. 9 Abs. 1 AI-DIAG), teilweise aber auch konkreter aus («Verlust, Entwendung sowie unrechtmässige[r] Bearbeitung und Kenntnisnahme», § 8 Abs. 1 BL-IDG; umfassender Katalog in § 7 Abs. 2 Bst. a–e ZH-IDG).

Grössere Unterschiede ergeben sich bezüglich weitergehender Pflichten. Wird die Datensicherheit verletzt, untersteht der Cloud-Provider einer Meldepflicht gegenüber dem öffentlichen Organ. Dieses hat unter bestimmten Bedingungen eine Meldepflicht gegenüber der Fachstelle Datenschutz und der betroffenen Person (z.B. Art. 9a SG-DSG). Zudem statuiert beispielsweise der Kanton Glarus, dass die Einhaltung der Datensicherheit durch den Cloud-Provider mittels Weisungen, Kontrollrechten, Auflagen, Vereinbarungen oder mittels anderer geeigneter Mittel durch die auslagernde Behörde sicherzustellen ist (Art. 6 Abs. 3 GL-DSG). Noch spezifischer geht der Kanton Freiburg vor, wenn er u.a. einen Vertrag zwischen der auslagernden Behörde und dem Cloud-Provider mit einem bestimmten Mindestinhalt vorschreibt (Art. 12c Abs. 1 Bst. b FR-DSchG).

Zusammenfassend ist die Einhaltung der Informationssicherheit eine der zentralen Pflichten der auslagernden Behörde und des Cloud-Providers. Dabei konzentrieren sich die **kantonalen Unterschiede besonders auf die weitergehenden Pflichten** wie Meldepflichten.

Datenschutzaudits

Die Einhaltung der Informationssicherheit (sowie anderer datenschutzrechtlicher Vorschriften) durch den Cloud-Provider ist durch die auslagernde Behörde zu kontrollieren. Generell enthalten jedoch nur die wenigsten kantonalen Datenschutzrechte Bestimmungen zu Datenschutzaudits. So ist eine Auslagerung nach einigen Datenschutzgesetzen nur dann zulässig, wenn die auslagernde Behörde Kontrollrechte gegenüber dem Cloud-Provider ungehindert ausüben kann (z.B. § 20 Abs. 2 Bst. c SZ-ÖDSG; Art. 9 Abs. 3 SG-DSG). In einigen Fällen wird zusätzlich gefordert, dass dies mittels Vertrag, Auflagen oder anderer Mittel zu erreichen ist (z.B. Art. 6 Abs. 3 GL-DSG; § 12a Abs. 1 Bst. g AG-VIDAG; § 13 Abs. 2 Bst. h LU-IG). Dabei ist gemäss dem Kanton Genf auch vertraglich zu vereinbaren, dass Audits auf dem Gelände des Cloud-Providers durchgeführt werden dürfen (Art. 13A Abs. 3 GE-RIPAD).

Insgesamt **beinhalten nur wenige kantonale Datenschutzrechte Regelungen über Datenschutzaudits,** deren Detaillierungsgrad wie in den Kantonen Luzern und Genf aber auch ausgesprochen hoch ausfallen kann.

AUTORIN

Nadine Rinderknecht,
ist Legal Trainee bei LAUX LAWYERS AG (www.lauxlawyers.ch) und Studentin der Universität Zürich.

IMPRESSUM

Verlag	WEKA Business Media AG Hermetschloostrasse 77 CH-8048 Zürich www.weka.ch
Herausgeber	Reto Fanger
Redaktion	Junes Babay
Publikation	10 × jährlich, Abonnement: CHF 98.– pro Jahr, Preise exkl. MWST und Versandkosten.
Layout/Satz	Dimitri Gabriel
Bildrechte	Autorenbilder: WEKA Business Media AG Alle übrigen Bilder: www.istockphoto.com
Bestell-Nr.	NL9231