www.jusletter-it.eu

Reto Fanger

Auswirkungen des revidierten Datenschutzgesetzes auf Cloudanbieter in der Schweiz

Das revidierte Schweizer Datenschutzgesetz (revDSG) wurde am 25. September 2020 verabschiedet und wird voraussichtlich am 1. September 2023 in Kraft treten, zusammen mit den ebenfalls revidierten Verordnungen zum Datenschutzgesetz (VDSG) und über die Datenschutzzertifizierungen (VDSZ). Dabei stellt sich die Frage, inwiefern sich die neuen Bestimmungen auf in- und ausländische Cloudanbieter in der Schweiz auswirken werden, zumal die Anpassung des Datenschutzrechts an die technologischen Herausforderungen ein zentrales Revisionsziel darstellte.

Beitragsart: Beiträge
Region: Schweiz
Rechtsgebiete: Datenschutz

Zitiervorschlag: Reto Fanger, Auswirkungen des revidierten Datenschutzgesetzes auf Cloudanbieter in der Schweiz, in: Jusletter IT 26. April 2022

Inhaltsübersicht

I. Ausgangslage

[1] Die Totalrevision des Schweizer Datenschutzgesetzes bezweckt, die angejahrten, auf Datenbearbeitungen von Privaten und der Bundesverwaltung anwendbaren Datenschutzbestimmungen des Bundes den rasanten technologischen, gesellschaftlichen sowie gesetzgeberischen Entwicklungen der letzten Jahre und Jahrzehnte anzupassen.[1]

[2] Das derzeit geltende DSG basiert auf dem am 19. Juni 1992 beschlossenen und am 1. Juli 1993 in Kraft getretenen Bundesgesetz über den Datenschutz (DSG), das diesen rasanten technologischen, gesellschaftlichen und gesetzgeberischen Veränderungen trotz Teilrevision (in Kraft seit 1. Januar 2008) nicht mehr standhalten konnte.[2]

[3] Startpunkt der Totalrevision war die Gutheissung des Berichts über die Evaluation des DSG durch den Bundesrat am 9. Dezember 2011 und die dabei erfolgte Auftragserteilung an das Eidgenössische Justiz- und Polizeidepartment (EJPD) zur Prüfung gesetzgeberischer Massnahmen zur Stärkung des Datenschutzes sowie zur Unterbreitung von Vorschlägen zum weiteren Vorgehen bis Ende 2014.[3]

[4] Der dadurch angestossene Revisionsprozess wurde, nach einigen Wendungen, mit der Verabschiedung des revidierten Datenschutzgesetzes (revDSG) am 25. September 2020 im Wesentlichen abgeschlossen.[4] Aktuell noch offen ist die Überarbeitung der zugehörigen Verordnung zum DSG (VDSG) sowie der Verordnung über die Datenschutzzertifizierungen (VDSZ), deren Referendumsvorlagen noch zu finalisieren sind.[5] Am 3. März 2022 teilte das Bundesamt für Justiz per Infobox auf seiner Website zur Datenschutzrevision und ohne weiteren Kommentar mit, es sei vorgesehen, das revidierte Datenschutzgesetz am 1. September 2023 in Kraft zu setzen; der

1 https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html; BBl 2017 6943.

2 https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de.

3 https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html; BBl 2017 6943 f./6954 f.

4 https://www.fedlex.admin.ch/eli/fga/2020/1998/de.

5 https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de; https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/vn-ber.pdf.download.pdf/vn-ber-d.pdf, S. 7.

dazu notwendige Bundesratsentscheid müsse noch erfolgen.[6] Geplant ist, das revDSG[7] gleichzeitig mit den bis dahin ebenfalls überarbeiteten Verordnungen VDSG und VDSZ in Kraft zu setzen.

II. Technikbezogene Revisionsziele

[5] Als erklärtes Revisionsziel sollte das schweizerische Recht an die rasante technologische Entwicklung mit ihren erheblichen Auswirkungen auf den Datenschutz angepasst werden:[8] Die Botschaft des Bundesrates aus dem Jahr 2017 erwähnte aus technologischer Sicht insbesondere die Wiedererlangung der Kontrolle über die Daten durch die Betroffenen, die Beschaffung von Personendaten im Zusammenhang mit der Entwicklung der digitalen Gesellschaft in sehr grosser Zahl (Big Data) und die immer intransparentere Bearbeitung, beispielsweise bei Profiling auf der Basis von Algorithmen. Gleichzeitig solle die Eigenverantwortung der Verantwortlichen gefördert werden, indem die Datenschutzvorschriften bei neuen Datenbearbeitungen bereits mit der Planung berücksichtigt und standardmässig die datenschutzfreundlichste Lösung vorzusehen sei.

III. Datenschutzrechtliche Aspekte des Cloud Computing

[6] Cloud Computing ist kein wirklich neuer Trend, dennoch steigt die Anzahl von Unternehmen weiterhin, die entweder mit ihrer IT gänzlich neu in die Cloud gehen oder es bereits seit Jahren sind, aber zusätzliche IT-Services dorthin verlagern.[9] Cloud Computing und damit die Nutzung externer IT-Dienstleistungen stellt als Outsourcing von Datenbearbeitungen ein Auftragsbearbeitungsverhältnis dar, das entweder *leistungsbezogen unterschieden* werden kann als

- *Software as a Service (SaaS)*, also der Nutzung der vom Dienstleister bereitgestellten Software bzw. Softwarefunktionalitäten durch den Kunden,
- *Infrastructure as a Service (IaaS)*, im Sinne einer Nutzung der vom Dienstleister bereitgestellten Komponenten einer virtualisierten Infrastruktur (beispielsweise als virtuelle Server etc.) durch den Kunden; dabei bleibt der Dienstleister für den Betrieb der eingesetzten Umgebung verantwortlich, der Kunde verwaltet die Komponenten selbst und implementiert die notwendigen Softwareinstallationen,
- *Platform as a Service (PaaS)*, in der Form der Bereitstellung von Entwicklungsumgebungen, auf denen der Kunde eigene Dienstleistungen entwickeln und betreiben kann, beziehungsweise
- *Business Process as a Service (BPaaS)* und somit einer digitalisierten Abbildung unternehmensspezifischer Geschäftsprozesse zur Erbringung hochstandardisierter Dienstleistungen,

6 https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html.

7 https://www.fedlex.admin.ch/eli/fga/2020/1998/de.

8 BBl 2017 6969.

9 Ralph Gramigna, Datenschutz und Outsourcing, in: Datenschutzrecht, Nicolas Passadelis/David Rosenthal/Hanspeter Thür (Hrsg.), Basel 2015, N 20.7 ff.; David Schwaninger/Michelle Merz, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke 2.0, in: Jusletter 21. Juni 2021, N 1.

oder *unterschieden nach den Liefermodellen* der

- *Private Cloud*, der Bereitstellung von Cloud-Dienstleistungen für die ausschliessliche Nutzung durch eine einzige Organisation,
- *Public Cloud* im Sinne einer Bereitstellung von Cloud-Dienstleistungen für eine Vielzahl voneinander unabhängiger Nutzende, beziehungsweise
- *Hybrid Cloud*, als Vereinigung der Leistungen sowie Aspekte von Private und Public Cloud.[10]

[7] Datenbearbeitung im Rahmen des Cloud Computing hat aus datenschutzrechtlicher Sicht insbesondere Risiken zu berücksichtigen wie Kontrollverlust, Datensicherheit, fehlende Portabilität, Isolierung verschiedener Datenbearbeitungen, Compliance Risiken sowie allfällige Zugriffe ausländischer Behörden.[11]

[8] Im Rahmen der Totalrevision des Datenschutzgesetzes mit erklärtem technikbezogenen Revisionsziel stellt sich daher die Frage, ob solche technikbezogenen Aspekte hinsichtlich des populären Phänomens des Cloud Computings und dessen spezifischen datenschutzrechtlichen Risiken Eingang in das revDSG gefunden haben.

IV. Gesetzgeberische Umsetzung der Revisionsziele

[9] Im Folgenden ist zu prüfen, welche Aspekte des revidierten Datenschutzgesetzes generell auf die von Auftragsbearbeitern für ihre Kunden erbrachten Dienstleistungen und somit spezifisch auch auf in- und ausländische Cloudanbieter in der Schweiz anwendbar sind.

1. Sachlicher Geltungsbereich/Personendaten

[10] In Anwendung von Art. 2 Abs. 1 gilt das revDSG für die Bearbeitung von Personendaten natürlicher Personen und somit für alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art 5 lit. a rev DSG). Dementsprechend entfällt der Schutz von Daten juristischer Personen nach dem bisherigen DSG, der bereits bisher keine grosse praktische Bedeutung hatte,[12] weshalb sich diese Verringerung des Scopes nicht merkbar auf Cloudanbieter auswirken wird. Für die Bestimmbarkeit einer natürlichen Person reicht – wie bereits nach geltendem Recht – die rein theoretische Möglichkeit *nicht* aus, dass jemand identifiziert werden kann; vielmehr bedarf es dabei einer Betrachtung der Gesamtheit der Mittel, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren, was mit Blick auf die konkreten Umstände (z.B. zeitlicher und finanzieller Aufwand für die Identifizierung) und damit einzelfallbezogen zu beurteilen ist: So gilt das Gesetz nicht für anonymisierte oder pseudonymisierte Daten, wenn eine Re-Identifizierung durch Dritte unmöglich ist oder nur mit einem grossen Aufwand möglich

10 Gramigna, a.a.O., N 20.7 f. m.w.H.; Schwaninger/Merz, a.a.O., N 1 u. 4.

11 Gramigna, a.a.O., N. 20.9; Schwaninger/Merz, a.a.O., N 1.

12 BBl 2017 7011.

wäre, den kein Interessent auf sich nehmen würde.[13] Dies entspricht auch der Rechtsprechung des Bundesgerichts im Fall «Logistep» aus dem Jahr 2010.[14]

2. Räumlicher Geltungsbereich

[11] Das revDSG gilt nach Art. 3 Abs. 1 für Sachverhalte, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden. Zunächst ist daher zu prüfen, ob bei einer Auslagerung von Personendaten an einen Cloudanbieter die Unterscheidung zwischen einer reinen «Schweizer Cloud» und einer «Cloud mit Auslandberührung» überhaupt sachgerecht ist:[15] Dies ist nicht der Fall, als das neue Datenschutzgesetz in Anwendung des räumlichen Geltungsbereichs von Art. 3 Abs. 1 revDSG für Sachverhalte gilt, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden. Dementsprechend ist das revidierte Datenschutzgesetz nicht nur auf die Cloudanbieter mit Sitz oder Niederlassung in der Schweiz anwendbar, sondern grundsätzlich auch auf diejenigen aus dem Ausland, sofern sie Personendaten aus der Schweiz bearbeiten (und sich diese Bearbeitung in der Schweiz auswirkt, was wohl für jegliche Bearbeitung von Personendaten im Cloudkontext zu bejahen ist). Abgesehen davon werden heute selbst Anbieter sogenannter «Schweizer Clouds» kaum ohne Auslandbezug Personendaten bearbeiten können; sei es, weil sich der Bezug zur Schweiz ohnehin nur an den «data at rest» und damit der Datenhaltung erschöpft, während die übrige Datenbearbeitung im Ausland stattfindet, oder weil selbst bei umfassenderem Bezug zur Schweiz durch die eingesetzten Unterlieferanten ein Auslandbezug nicht vermieden werden kann, und sei es nur für den Supportfall und entsprechender Einsicht in Klardaten.

[12] Die explizite gesetzliche Regelung des räumlichen Geltungsbereiches ist neu, nicht aber dessen Auswirkungen: So besteht bereits nach geltendem DSG aufgrund der Auswirkungstheorie die Möglichkeit, die gesetzlichen Bestimmungen auf Situationen mit internationalem Charakter anzuwenden, was durch das Bundesgericht im Entscheid «Google Street View» bestätigt wurde.[16] Ab welchem Ausmass solcher Auswirkungen von einer Anwendbarkeit auszugehen ist, bleibt unklar, auch wenn es sich dabei um Auswirkungen handeln muss, die über den Einzelfall hinausgehen und spürbare tatsächliche Einwirkungen in die Persönlichkeit der betroffenen Person in der Schweiz zeitigen, während bloss potentielle Auswirkungen wohl nicht reichen.[17] Trotz Anwendbarkeit des revDSG ergeben sich im Regelfall bei Sachverhalten mit internationalem Charakter oftmals Schwierigkeiten in der Umsetzung und Vollstreckung von Entscheiden,[18] was für den Fall des über den Sitz oder die Zweigniederlassung in der Schweiz lokalisierten Cloudanbieters, der ausländische Services und Tools in seine Dienstleistungen integriert nicht zutreffen dürfte, da er diesbezüglich als Verantwortlicher selber in der Pflicht zur Einhaltung des revDSG steht und auch bei Nichteinhaltung künftig verwaltungs-, straf- oder zivilrechtlich sanktioniert werden kann.

13 BBl 2017 7019; David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, N 20.

14 BGE 136 II 508 E. 3.

15 Schwaninger/Merz, a.a.O., N 6 ff.

16 BBl 2017 7017; BGE 138 II 346 E. 3.3.

17 Rosenthal, a.a.O., N 88.

18 BBl 2017 7017.

3. Bekanntgabe ins Ausland

[13] Folglich stellen sich dem Anbieter von Cloud-Lösungen in der Schweiz, zumal er aufgrund des räumlichen Geltungsbereichs mit der Anwendbarkeit des revDSG ausgehen muss, in aller Regel Fragen zur Datenbekanntgabe ins Ausland nach den Art. 16 ff. revDSG. Handelt es sich beim Auslandbezug um Länder, die keinen angemessen Schutz gewährleisten können, sind die entsprechenden Risiken gar vertieft zu prüfen und gegebenenfalls einzelfallweise entsprechende Massnahmen wie der Abschluss vertraglicher Regelungen (beispielsweise der Standard Contract Clauses, SCC) bzw. allfällige zusätzliche Massnahmen (wie Anonymisierung oder Verschlüsselung der Datensätze) zu ergreifen: Das zu wählende Vorgehen bei dieser Prüfung hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) im Rahmen seines Merkblatts «Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug (nach Art. 6 Abs. 2 lit. a DSG)» vom 18. Juni 2021 festgelegt[19] und ist in der aktuellen Form analog bzw. künftig angepasst an die Bestimmungen des revDSG direkt anwendbar.

4. Auftragsbearbeitung

[14] Das Verhältnis des Cloudanbieters zu seinem Kunden ist aus datenschutzrechtlicher Sicht klassischerweise dasjenige einer Auftragsbearbeitung:[20] Als Auftragsbearbeiter nach Art. 5 lit. k revDSG gilt die private Person oder das Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet. Die Bearbeitung von Personendaten kann gemäss Art. 9 Abs. 1 revDSG vertraglich oder durch Gesetzgebung dem Auftragsbearbeiter übertragen werden, sofern dieser die Daten so bearbeitet, wie der Verantwortliche dies tun dürfte (lit. a) und keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet (lit. b).

5. Datensicherheit

[15] Das Datensicherheitskonzept des revDSG beruht auf drei Säulen, von denen aber nur der Grundsatz der Datensicherheit nach Art. 8 DSG (direkt) verpflichtende Wirkung für den Auftragsbearbeiter und damit auch den Cloudanbieter hat.

5.1. Datenschutz durch Technik

[16] Die Grundidee der Pflicht zum Datenschutz durch Technik (Privacy by Design) besteht darin, dass sich Technik und Recht gegenseitig ergänzen sollen und dabei nicht auf eine bestimmte Technologie abgezielt wird:[21] Vielmehr sollen Systeme zur Datenbearbeitung technisch und organisatorisch so ausgestaltet sein, dass dieses die Gefahr von Verstössen gegen Datenschutzvorschriften reduziert oder ausschliesst, beispielsweise durch implementierte Regeln zur Datenlöschung oder standardisierter Anonymisierung. Dies ist so einleuchtend wie praktisch schwierig

19 https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/Anleitung.pdf.

20 Schwaninger/Merz, a.a.O., N 2; Gramigna, a.a.O., N 20.18 ff.

21 BBl 2017 7029.

umzusetzen und wohl auch nicht zu kontrollieren.[22] Der Verantwortliche ist zwar nach Art. 7 Abs. 1 revDSG verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Bearbeitungsgrundsätze nach Artikel 6 revDSG; er berücksichtigt dies ab der Planung.

[17] Die technischen und organisatorischen Massnahmen müssen gemäss Art. 7 Abs. 2 revDSG insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein. Mit diesem risikobasierten Ansatz muss das Risiko, das mit einer Bearbeitung einhergeht, in Beziehung gesetzt werden zu den technischen Möglichkeiten, um dieses zu verringern. Je höher das Risiko, je grösser die Eintrittswahrscheinlichkeit und je umfangreicher die Datenbearbeitung, desto höher müssen die Anforderungen an die technischen Vorkehren sein, um als angemessen gelten zu können.[23]

[18] Sanktioniert werden kann der Verantwortliche, mit Ausnahme von Verwaltungsmassnahmen des EDÖB im Sinne von Art. 51 revDSG, allerdings nicht.[24] Wie bereits erwähnt, richtet sich die Bestimmung nur an den Verantwortlichen und nicht an den Auftragsbearbeiter, weshalb der Cloudanbieter nur in dieser Rolle unter die Bestimmung fällt.

5.2. Datenschutz durch datenschutzfreundliche Voreinstellung

[19] Der Verantwortliche – und wiederum nur er, nicht der Auftragsbearbeiter – ist nach Art. 7 Abs. 3 revDSG verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt (Privacy by Default).[25] Dabei handelt es sich insbesondere um die Voreinstellungen von Software, die entsprechend datenschutzfreundlich auszugestalten sind, sofern keine abweichende Eingabe durch den Nutzer erfolgt.[26] Nachdem auch Art. 7 Abs. 3 revDSG nur auf den Verantwortlichen anwendbar ist, bezieht sich dessen Relevanz ebenfalls nicht auf das Auftragsbearbeitungsverhältnis zum Kunden, sondern nur auf die datenschutzrechtliche Stellung des Cloudanbieters in seiner Funktion als Verantwortlicher.

5.3. Datensicherheit im engeren Sinne

[20] Gestützt auf Art. 8 Abs. 1 f. revDSG müssen sowohl der Verantwortliche wie auch der Auftragsbearbeiter eine dem Risiko angemessene Datensicherheit durch geeignete technische und organisatorische Massnahmen gewährleisten. Dabei müssen die Massnahmen ermöglichen, Verletzungen der Datensicherheit zu vermeiden. Massgebend ist ebenfalls der risikobasierte Ansatz, wonach grössere Risiken umfangreichere Massnahmen nach sich ziehen müssen.[27] Sie umfassen den allgemeinen technischen und organisatorischen Rahmen der Datenbearbeitung beim Verant-

22 Rosenthal, a.a.O., N 43.

23 BBl 2017 7029 f.

24 Rosenthal, a.a.O., N 43.

25 Art. 7 Abs. 3 revDSG.

26 BBl 2017 7030.

27 BBl 2017 7031.

wortlichen oder Auftragsbearbeiter und gehen damit über die reine Bearbeitung von Personendaten hinaus.[28]

[21] Im Grundsatz entsprechen die Bestimmungen des revDSG zu den technischen und organisatorischen Massnahmen (TOM) dem bisherigen Recht. Neu ist hingegen, dass die vorsätzliche Verletzung von Art. 8 in Verbindung mit Art. 61 lit. c revDSG künftig mit Busse bis maximal CHF 250'000 strafrechtlich sanktioniert werden kann. Die erwähnten Mindestanforderungen im Sinne von Art. 8 Abs. 3 bzw. Art. 61 lit. c revDSG sind vom Bundesrat im Rahmen der noch nicht abgeschlossenen Revision der VDSG noch zu erlassen.[29]

6. Verzeichnis der Bearbeitungstätigkeiten

[22] Neben den Verantwortlichen müssen auch Auftragsbearbeiter gemäss Art. 12 Abs. 3 revDSG ein Verzeichnis der Bearbeitungstätigkeiten erstellen, das allerdings lediglich Angaben zur Identität des Auftragsbearbeiters und des Verantwortlichen, zu den Kategorien von Bearbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden, zu den Massnahmen der Datensicherheit (im Sinne einer allgemeinen Beschreibung) sowie bei Auslandbekanntgabe zum Zielstaat und zu allenfalls erforderlichen Garantien zur Gewährleistung des Datenschutzes für unsichere Drittstaaten. Letztlich handelt es sich dabei um eine verkürzte Liste der Mindestangaben,[30] die der Cloudanbieter als Verantwortlicher nach Art. 12 Abs. 2 revDSG ohnehin zu erstellen hat, wenn auch als separates Verzeichnis. Dies immer unter der Voraussetzung, dass der Cloudanbieter sowohl als Verantwortlicher wie auch als Auftragsbearbeiter nicht unter die Ausnahme von Art. 12 Abs. 5 revDSG fällt: Diese Ausnahmebestimmung dürfte allerdings für den konkreten Anwendungsfall des Cloudanbieters keine Rolle spielen, da die kumulativ zur Mitarbeiteranzahl (unter 250) zu erbringende Anforderung eines geringen Risikos von Verletzungen der betroffenen Personen kaum je zutreffen wird.

7. Meldung der Verletzung der Datensicherheit

[23] Bei Verletzungen der Datensicherheit hat der Auftragsbearbeiter diese nach Art. 24 Abs. 3 revDSG dem Verantwortlichen so rasch als möglich zu melden. Diese Meldepflicht des Auftragsbearbeiters geht weiter als diejenige des Verantwortlichen, da er jede Verletzung der Datensicherheit, von der er Kenntnis erhält, so rasch als möglich dem Verantwortlichen melden muss[31] – unabhängig davon, ob die Verletzung ein Risiko mit sich bringt, wie es die Anforderung an den Verantwortlichen von Art. 24 Abs. 1 revDSG festsetzt.

[24] Bei dieser Meldepflicht des Auftragsbearbeiters handelt es sich um eine gesetzliche Verpflichtung, weshalb sie keiner vertraglichen Vereinbarung mit dem Verantwortlichen bedarf und auch vertraglich nicht wegbedungen werden kann.[32] Unbesehen dieser Verpflichtung, ist deren Unterlassung oder Verzögerung strafrechtlich nicht sanktioniert, kann aber allenfalls Schadenersatz-

28 BBl 2017 7031; Rosenthal, a.a.O., N 53.

29 Rosenthal, a.a.O., N 56.

30 BBl 2017 7037.

31 BBl 2017 7065.

32 Rosenthal, a.a.O., N 165.

forderungen des Verantwortlichen nach sich ziehen, aufgrund gänzlich unterlassener, zu spät oder unvollständig erfolgter Meldungen.[33]

V. Fazit

[25] Zusammenfassend steht fest, dass die Bestimmungen des revDSG für inländische oder ausländische Cloudanbieter in der Schweiz keine bahnbrechenden Neuerungen mit sich bringen werden. Als Ausnahme dieser Feststellung kann die neu eingeführte Strafbarkeit bei vorsätzlicher Verletzung der Datensicherheit nach Art. 8 revDSG gelten (wobei Eventualvorsatz genügt). Die zur Einhaltung von Art. 8 revDSG zu beachtenden technischen und organisatorischen Massnahmen muss der Cloudanbieter allerdings bereits heute bereitstellen, weil er aufgrund seiner geschäftlichen Ausrichtung allenfalls dem Anwendungsbereich der DSGVO unterstellt und/oder durch seine Kunden vertraglich zur Einhaltung technischer und organisatorischen Massnahmen nach dem aktuellen Stand der Technik verpflichtet ist sowie – last but not least – sich grundsätzlich im Rahmen seiner auftragsbezogenen- oder werkvertraglichen Dienstleistung ohnehin zur Sorgfalt verpflichtet sieht. Mit Abstrichen angeführt werden kann überdies noch die strenge Meldepflicht des Auftragsbearbeiters nach Art. 24 Abs. 3 revDSG, deren Nichteinhaltung, Verzögerung oder Unvollständigkeit Schadenersatzforderungen des Verantwortlichen gegenüber dem Cloudanbieter zur Folge haben kann.

Reto Fanger, Dr. iur., Rechtsanwalt, Gründer und Inhaber ADVOKATUR FANGER, Luzern, Lehrbeauftragter an der Richterakademie der Universität Luzern und Dozent an der Hochschule Luzern.

33 Rosenthal, a.a.O., N 167.