Stand 25.9.2020

VUD Verein Unternehmens-Datenschutz

Rohstoff zum revidierten Datenschutzgesetz*

In Kürze

- Neue Informations- und Dokumentationspflichten → Anpassen und Erstellen
- Bussenrisiko u.a. bei Auslandstransfers und bestimmten Service-Verträgen → Überprüfen
- Meldepflicht bei Datenverlusten und sonstigen Sicherheitspannen → Prozess einführen
- Neues DSG meist nicht strenger als DSGVO, aber nicht identisch → Differenzen prüfen

Eckpunkte der Revision

1. Das neue DSG tritt wohl nicht vor **2022** in Kraft; einige rechnen erst mit Sommer 2022
2. Die **Grundprinzipien** des Datenschutzes ändern sich nicht; Einwilligungen für das Bearbeiten von Personendaten sind nach wie vor meist keine erforderlich (anders als unter der DSGVO)
3. Hinzugekommen sind mehr oder weniger aufwändige **Governance-Pflichten**, wie das Führen von Datenbearbeitungs-Inventaren, eine Meldepflicht von Datenverlusten und anderen Sicherheitsverstössen und die Pflicht zur Vornahme von Datenschutz-Folgenabschätzungen
4. Neu ist vorgesehen, dass Unternehmen **Datenschutzberater** ernennen können und ausländische Unternehmen mit wesentlichen Aktivitäten in der Schweiz eine **Schweizer Vertretung** bestimmen müssen
5. Die **Rechte der betroffenen Personen** werden etwas ausgebaut; es wird noch einfacher, die eigenen Daten von einem Unternehmen herauszuverlangen
6. **Verträge** müssen auf DSG-Konformität überprüft werden; namentlich bei sog. Auftragsbearbeitern wird der Beizug von Subakkordanten strenger geregelt (analog DSGVO)
7. **Profiling** stand zwar im Zentrum der Diskussion, aber es ändert sich kaum etwas
8. **Informationspflicht** bei Datenbeschaffungen wird inhaltlich (d.h. worüber informiert werden muss) ausgeweitet; Unternehmen müssen daher ihre Datenschutzerklärungen überprüfen
9. Der **Auslandstransfer** von Daten wird zwar liberalisiert, aber Verstösse sind neu strafbewehrt
10. Bearbeitung von Daten zur **Prüfung der Kreditwürdigkeit** wird insb. zeitlich eingeschränkt
11. Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte kann neu **Bearbeitungsverbote** und andere Verfügungen erlassen und nicht mehr nur «Empfehlungen»
12. Die **Strafbestimmungen** (CHF 250'000) zielen auf verantwortliche Mitarbeiter, nicht Firmen, betreffen aber nur wenige Fälle (Information, Auskunft, Exporte, Sicherheit, Outsourcing)
13. Wer **DSGVO-konform** ist wird mit einigen Ausnahmen auch DSG-konform sein; Daten über juristische Personen sind aber nicht mehr im Geltungsbereich

Handlungsbedarf

1. Datenschutzerklärungen auf die neuen Vorgaben hin überprüfen und anpassen; prüfen, ob alle Fälle abgedeckt sind, wo das Unternehmen Personendaten beschafft
2. Verzeichnis der Datenbearbeitungen erstellen
3. Auftragsbearbeitungen identifizieren und Verträge auf Vorgaben hin prüfen und anpassen
4. Auslandstransfers identifizieren und auf Vorgaben hin prüfen und anpassen
5. Prozess für Datenschutz-Folgenabschätzung einführen, ev. Datenschutzberater ernennen
6. Prozess zur Meldung und Bearbeitung von Verletzungen der Datensicherheit einführen
7. Vorgaben zur Beantwortung von Ersuchen betroffener Personen erstellen oder anpassen
8. Automatisierte Einzelentscheide identifizieren und bei Relevanz ggf. neu regeln
9. Bearbeitungen von genetischen und biometrischen Daten sowie für nicht personenbezogene Zwecke und Kreditwürdigkeit identifizieren, auf neue Vorgaben hin prüfen und anpassen
10. Schulungen und Weisungen anpassen, Audits vorsehen

Stand 25.9.2020

Häufige Fragen und Antworten

Wie ist der weitere Fahrplan?

Das revidierte Datenschutzgesetz wurde am 25. September 2020 von den Räten verabschiedet. Mit einem Inkrafttreten wird nicht vor 2022 gerechnet; in Bundesbern gibt es diverse Stimmen, die eine Inkraftsetzung sogar erst im Sommer 2022 erwarten. Der Fahrplan hängt einerseits vom Druck ab, den die EU mit Bezug auf die Erneuerung des Angemessenheitsbeschlusses der Europäischen Kommission auf die Schweiz aufsetzt, und andererseits von den weiteren Arbeiten. Es ist geplant, wohl im 1. Quartal 2021 den Entwurf für die revidierten Verordnungen zur öffentlichen Vernehmlassung aufzulegen. Relevante Übergangsfristen hat das neue DSG selbst keine (sie wurden gestrichen).

Schlussabstimmungstext: https://www.parlament.ch/centers/eparl/curia/2017/20170059/Schluzss-abstimmungstext%203%20NS%20D.pdf

Synoptische Darstellung und englische Übersetzung: https://datenrecht.ch/dsg-revision/

Müssen auch jene, die die DSGVO bereits umgesetzt haben, etwas unternehmen, um für das neue DSG fit zu sein?

Ja, denn in gewissen Bereichen enthält das DSG abweichende oder weitergehende Regeln, aber im Grossen und Ganzen sind DSGVO-konforme Unternehmen gut aufgestellt.

Im Bereich der Informationspflicht müssen die Länder angegeben werden, in welche Daten übermittelt werden können, und es müssen andere als unter der DSGVO verlangten Angaben zu den hierzu getroffenen Vorkehrungen gemacht werden (dies kann jedoch mit wenigen Worten erfüllt werden und statt einer Länderliste sind auch Bezeichnungen wie "Europa" möglich). Dies bedeutet, dass Datenschutzerklärungen angepasst werden müssen. Es muss sichergestellt werden, dass Anfragen von Betroffenen (z.B. Auskunftsgesuche) nach den Kriterien des DSG geprüft werden, die von jenen der DSGVO abweichen. Das DSG ist dabei teilweise strenger als die DSGVO: Geschäftsgeheimnisse können nicht so gut wie unter der DSGVO vor Einsichtnahme geschützt werden.

Bei den Datenexporten geht das neue DSG zwar ähnliche Wege wie die DSGVO, aber die damit verbundenen Melde- bzw. Genehmigungspflichten sind anders und müssen separat beurteilt werden. Das gilt auch für Verletzungen der Datensicherheit: Die Meldepflicht ist in der Schweiz anders geregelt als unter der DSGVO. Verträge mit Auftragsbearbeitern müssen ebenfalls allenfalls angepasst werden, weil sie sich nicht nur auf die DSGVO beziehen dürfen – grundsätzlich ändert sich jedoch nichts.

Zu beachten ist schliesslich, dass gewisse ausländische Unternehmen in der Schweiz einen Vertreter ernennen müssen. Ein Datenschutzberater ist jedoch nicht Pflicht.

Welche Massnahmen werden den grössten Aufwand mit sich bringen?

Den grössten Aufwand bringt erfahrungsgemäss das Erstellen der Dokumentation (Verzeichnis der Datenbearbeitungen, Datenschutz-Folgenabschätzungen), die Durchsicht von Verträgen zum Datenschutz sowie die generelle Prüfung der diversen Datenbearbeitungen auf ihre Konformität mit dem revidierten DSG mit. Das neue DSG schreibt zwar die Dokumentation nicht wie die DSGVO vor (kein Pendant zum Prinzip der «Accountability»), aber eine gute Governance und «Privacy by Design» verlangt sie oft trotzdem. Die Schulung der Mitarbeiter kann ebenfalls viel Zeit beanspruchen.

Das Erstellen der Datenschutzerklärungen braucht erfahrungsgemäss einigen Aufwand, und zwar nicht, weil solche zu schreiben besonders kompliziert wäre, sondern weil das Unternehmen zunächst

überhaupt verstehen muss, wo es welche Personendaten zu welchen Zwecken intern und extern beschafft, wie es diese bearbeitet und wem es sie weitergibt. Dabei muss bei der Zusammenarbeit mit Dienstleistern, die Daten bearbeiten, auch deren datenschutzrechtliches Verhältnis zum Unternehmen bestimmt werden (sind sie lediglich «Auftragsbearbeiter» oder aber eigenständige oder gemeinsame «Verantwortliche»?). Das kann schwierige Abgrenzungsfragen aufwerfen und die Antworten können Auswirkungen auch auf die Verträge haben (d.h. diese müssen ggf. auch angepasst werden). Wo Unternehmen diese Abklärungen schon unter altem Recht oder für die DSGVO unternommen haben, ist die Anpassung der Datenschutzerklärung (und Verträge) relativ einfach.

Die für das neue DSG nötigen Prozesse (Auskunftsersuchen, Einführung neuer Projekte, Datenpannen) zu definieren, dürfte in aller Regel nicht sehr viel Zeit beanspruchen, da viele der Prozesse im Ansatz schon bestehen. Es müssen jedoch unterschiedliche Stellen (z.B. Kundendienst, Fachbereiche, Medienstelle, Informatik, Information Security, Regulatory Affairs, Geschäftsleitung) involviert werden und es muss dies frühzeitig geschehen, weil jederzeit mit Verletzungen der Datensicherheit oder Anfragen von Betroffenen gerechnet werden kann, die dann zu bearbeiten sind.

Die Informationspflicht ist laut DSG umfassend – das lässt sich doch gar nicht erfüllen!

Das ist richtig. Der Gesetzgeber hat es sich hier einfach gemacht; das Parlament dachte zwar über zusätzliche Einschränkungen nach, gab diese aber auf, weil es befürchtete, dadurch nicht EU-kompatibel zu sein. Immerhin geht die Informationspflicht (Art. 19 revDSG) nicht ganz so weit wie unter der DSGVO (z.B. weniger Pflichtinformationen im Giesskannenprinzip) und es gibt relativ viele Ausnahmebestimmungen (z.B. auch für alle gesetzlich vorgeschriebenen Bearbeitungen, wie etwa beim Personaldossier). Zudem gilt die Informationspflicht nicht für jede Datenbearbeitung, sondern nur für Fälle, in denen Daten planmässig beschafft werden. Die vorsätzliche Verletzung der Informationspflicht ist allerdings bussenbewehrt.

In der Praxis gehen Unternehmen damit so um, dass sie erstens umfassende Datenschutzerklärungen auf ihren Websites publizieren, sie zweitens in AGB und anderen Dokumenten auf diese hinweisen und drittens darauf achten, dass bei Kontakten mit betroffenen Personen diese mindestens gewisse Basisinformationen erhalten oder erkennen können, wer von ihnen wozu Daten erhebt und wo es weiterführende Hinweise gibt.

Gibt es das «Recht auf Vergessen» aus der DSGVO in der Schweiz nun ebenfalls?

Das gab es schon immer und gibt es weiterhin. Es ist im DSG bloss nicht so bezeichnet. Wie unter der DSGVO ist der Löschanspruch auch in der Schweiz nicht absolut, d.h. es muss nicht einfach diskussionslos gelöscht werden, wenn eine betroffene Person das verlangt. Besteht ein überwiegendes Interesse (oder sogar eine gesetzliche Pflicht), gewisse Daten weiterhin aufzubewahren, so darf das getan werden.

Den Grundsatz der Verhältnismässigkeit gab es freilich schon immer und wird im neuen DSG noch deutlicher zum Ausdruck gebracht: Personendaten dürfen nur solange aufbewahrt wie wirklich nötig, und zwar nur jene Daten, die es wirklich braucht. Auch der Zugang muss «need to know» sein. Anstatt dass Daten gelöscht werden, genügt es auch sie zu anonymisieren.

Ist «Profiling» jetzt überhaupt noch erlaubt oder nur mit Einwilligung?

Profiling ist rechtlich weiterhin meistens ohne Einwilligung erlaubt. Hier weicht die öffentliche Diskussion und Wahrnehmung vom Gesetz ab (was allerdings Erwartungshaltungen seitens der Konsumenten und Behörden wecken kann). Das Parlament stritt über die Legaldefinition des Profilings und vor allem der Untervariante des Profilings «mit hohem Risiko», obwohl keine einzige Bestimmung im

neuen DSG eine Einwilligung für Profiling erfordert. Das DSG sagt nur, dass soweit in der Privatwirtschaft für ein Profiling «mit hohem Risiko» auf eine Einwilligung abgestellt wird, diese eine ausdrückliche sein muss (bei Bundesorganen gilt das für jedes Profiling). Die einzige Einschränkung für das Profiling im neuen DSG ist, dass Wirtschaftsauskunfteien sich bei einer Bearbeitung von Daten zur Kreditwürdigkeit einer Person nicht auf Daten aus einem Profiling «mit hohem Risiko» abstützen dürfen, wenn diese das nicht will, und für Bundesorgane eine Grundlage in einem formellen Gesetz (statt in einem beliebigen Erlass) nötig ist. Ungeachtet dessen gilt, was immer galt: Je heikler die Datenbearbeitung ist, je höher die Risiken für eine betroffene Person sind, desto höher die Anforderungen an den Datenschutz. Das ist natürlich auch beim Profiling zu beachten. Geht ein Profiling sehr weit, so kann es gegen Treu und Glauben bzw. den Grundsatz der Verhältnismässigkeit (insbesondere bezüglich Zumutbarkeit für die betroffene Person) verstossen, dadurch die Persönlichkeit verletzen und in diesem konkreten Fall eine Rechtfertigung erfordern; die Einwilligung ist dann eine von mehreren Wegen zur Rechtfertigung. Natürlich gilt auch, dass in solchen – aber auch allen anderen Fällen von heiklen Datenbearbeitungen – eine Datenschutz-Folgenabschätzung und eine erhöhte Transparenz nötig sein kann.

Und was ist Profiling und Profiling mit einem hohen Risiko überhaupt?

Profiling ist im Wesentlichen eine maschinelle Bewertung eines Individuums, eine Art automatisierte Meinungsbildung oder Interpretation bestimmter Aspekte einer Person. Ein manuelles Profiling im Sinne des DSG gibt es also nicht. Es geht darum, dass ein Computer alleine einen Wertentscheid trifft, auch wenn er das in aller Regel nach der genauen Vorgabe eines Menschen tut. Das grenzt sich ab zur Feststellung des Sachverhalts, wo kein Ermessen und keine Interpretation im Spiel ist (also kein «bewerten») und es daher aus Sicht des Gesetzgebers auch nicht problematisch erscheint, dass ein Computer und nicht ein Mensch dies tut. Wenn also der Weinhändler von seinem Computer eine Liste von all den Kunden für ein Mailing für eine neue Weinlieferung selektieren lässt, die bisher Weine einer bestimmten Sorte bestellt haben, so liegt ein Profiling vor: Es ist dies ein von einem Computer aufgrund bisheriger Bestellungen ausgeführter Wertentscheid (i.c. eine Prognose) bezüglich der Frage, welcher der Kunden sich für die neue Weinlieferung wohl besonders interessieren werden.

Ein Profiling «mit hohem Risiko» verlangt demgegenüber mehr. Das Ergebnis muss aufgrund einer Verknüpfung von Daten eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben und dadurch ein hohes Risiko der Persönlichkeitsverletzung mit sich bringen. Damit greift die Definition den schon bisher bekannten Begriff des Persönlichkeitsprofils auf. Ein Profiling mit hohem Risiko ist also vereinfacht gesagt ein Profiling, das zu einem Persönlichkeitsprofil führt, das heikel ist. Das wäre im vorgenannten Beispiel nicht der Fall.

Muss jetzt für alles eine Einwilligungserklärung eingeholt werden?

Nein, obwohl hierbei viele verunsichert sind. Schon das bisherige DSG verlangte grundsätzlich keine Einwilligung der betroffenen Person, damit Daten bearbeitet werden dürfen. Das DSG weicht dabei deutlich von der DSGVO ab, indem es für die Bearbeitung von Personendaten durch private Stellen zwar insbesondere die Einhaltung der Bearbeitungsgrundsätze erfordert und dass ein etwaiger Widerspruch der betroffenen Person beachtet wird, aber keine «Rechtsgrundlage» verlangt (also gezeigt werden muss, dass z.B. ein berechtigtes Interesse vorliegt, eine Einwilligung besteht, die Bearbeitung der Vertragsabwicklung dient oder der Einhaltung von EU-Recht). Am bisherigen Regulierungskonzept des DSG ändert sich also nichts. Eine Einwilligung kann immerhin eine ansonsten persönlichkeitsverletzende Datenbearbeitung rechtfertigen (also, wenn die Bearbeitungsgrundsätze nicht eingehalten werden, wie z.B. Zweckbindung, Verhältnismässig, Transparenz und Datenrichtig-

keit). Auch bei der Weitergabe von besonders schützenswerten Personendaten ist eine Rechtfertigung zwingend erforderlich (die allerdings nicht eine Einwilligung sein muss; denkbar ist z.B. auch der Rechtfertigungsgrund der Vertragsabwicklung). Die Bestimmung zur Einwilligung in Art. 6 revDSG ist daher als reine Begriffsdefinition und nicht als Pflicht zu verstehen, d.h. sie sagt nur, dass eine Einwilligung ausdrücklich erfolgen muss, falls sie für die Bearbeitung von besonders schützenswerten Personendaten oder für ein Profiling «mit hohem Risiko» gültig eingeholt werden soll.

Zu beachten ist immerhin, dass andere Gesetze teilweise eine Einwilligung erfordern können, z.B. Art. 3 Abs. 1 Bst o UWG (Werbemails) oder Geheimhaltungspflichten (zwecks Waiver, z.B. Art. 321 StGB, Art. 47 BankG). Auch der «gefühlte» Datenschutz kann es erforderlich machen bzw. zur Erwartungshaltung führen, dass eine Einwilligung eingeholt wird, selbst wenn dies streng genommen nicht nötig wäre. Dasselbe gilt für die Frage, ob die Einwilligung für bestimmte Aktivitäten (z.B. Marketing) separat eingeholt werden muss (damit sie als freiwillig gilt). Unter der DSGVO ist dies viel eher der Fall, als unter dem DSG.

Erfordert das neue Gesetz die Bestellung eines betrieblichen «Datenschutzbeauftragten», wie ihn die DSGVO teilweise verlangt?

Jein. Das DSG sieht anders als die DSGVO keine Pflicht zur Bestellung einer betrieblichen Datenschutzstelle vor. In der Praxis werden Unternehmen ab einer gewissen Grösse jedoch nicht mehr ohne eine Stelle bzw. Person, die für den Datenschutz zuständig ist, auskommen können. Faktisch ist eine solche Stelle darum in vielen Unternehmen erforderlich (und bereits bestellt). Weil aber keine gesetzliche Pflicht besteht, besteht mehr Flexibilität in der Ausgestaltung der Stelle.

Unternehmen sollten sich überlegen, diese Stelle trotzdem nach den Vorgaben des neu geschaffenen «Datenschutzberaters» (so der neue Terminus im revidierten DSG) auszugestalten (d.h. punkto Unabhängigkeit, Interessenkonflikte, Fachwissen), weil sie dann den Vorteil haben, dass bei meldepflichtigen Datenschutz-Folgenabschätzungen sie nicht zum Eidg. Datenschutz- und Öffentlichkeitsbeauftragten gehen müssen. Dies ist aber zugegeben kein besonders grosser Anreiz.

Gewisse ausländische Unternehmen werden ferner einen «Vertreter» in der Schweiz ernennen müssen (der dann als Anlaufstelle für betroffene Personen und den EDÖB im Inland fungiert). Dies kann auch eine Schweizer Tochtergesellschaft sein. In beiden Fällen (Datenschutzberater, Vertreter) müssen die Kontaktdaten publiziert werden.

Was hat es mit dem Schlagwort «Privacy by Design» und «Privacy by Default» auf sich?

Die Pflicht zum «Privacy by Design» gab es schon bisher, weil Datenbearbeitungen schon bisher so ausgestaltet sein mussten, dass das DSG eingehalten wird bzw. werden kann. Das verlangt auch Privacy by Design. Dies ist somit keine Neuerung. Es bedeutet, dass Unternehmen sich von Anfang an bei Aktivitäten, die zu einer Datenbearbeitung führen, Gedanken über den Datenschutz machen und passende Vorkehrungen treffen sollten – an sich eine Selbstverständlichkeit.

Die Pflicht zum «Privacy by Default» bedeutet, dass dort, wo im Rahmen einer Onlineanwendung oder sonst einer Datenbearbeitung mit Voreinstellungen zum Datenschutz gearbeitet wird, die der Benutzer später ändern kann, sie standardmässig die datenschutzfreundlichste Einstellung aufweisen sollen. Das bedeutet aber nicht, dass Benutzer von Anfang an gefragt werden können, welche Einstellungen sie wollen und ein Kästchen dabei nicht schon vorangekreuzt sein darf.

Was bedeutet das neue Recht der «Datenportabilität»?

Dieses Recht wurde für die DSGVO erfunden und im Rahmen der Parlamentsdebatte im Zuge eines Kompromisses auch in der Schweiz eingeführt. Es soll Benutzern speziell von Online-Diensten erleichtern, die über sie gesammelten Daten von einem Dienstleister (z.B. eine Playlist) zu einem anderen zu verschieben und so einfacher zwischen Dienstleistern zu wechseln. Es wird sich auch unter der DSGVO noch zeigen müssen, wo es wirklich eine Rolle spielt. Technisch gesehen ist es allerdings extrem breit formuliert und greift im Grunde überall dort, wo Unternehmen für ein Vertragsverhältnis in eigener Verantwortung elektronisch Daten der betroffenen Personen (als ihre Vertragspartner) sammeln. Solche Daten kann die betroffene Person elektronisch herausverlangen. Es wird befürchtet, dass dies teilweise so weit geht, dass z.B. ein Mitarbeiter von seinem Arbeitgeber die Herausgabe seiner geschäftlichen E-Mailbox verlangen kann. Was genau hinter diesem neuen Recht steckt, wird die Praxis also noch zeigen müssen.

Wenn Daten juristischer Personen vom DSG nicht mehr erfasst sind, sind diese damit nicht mehr geschützt?

Doch, sie sind weiterhin in gewissem Umfang geschützt. Zunächst haben sie (weiterhin) Anspruch auf den Schutz ihrer Persönlichkeit, z.B. wenn sie bezüglich ihrer Kreditwürdigkeit unberechtigterweise verunglimpft werden. Das war mit Art. 28 ZGB schon vor dem DSG so und ist es auch weiterhin. Da das DSG Art. 28 ZGB konkretisiert, darf damit gerechnet werden, dass seine Bearbeitungsgrundsätze mit Bezug auf Daten juristischer Personen analog angewendet werden. Allerdings gelten Daten juristischer Personen schon heute als weniger sensibel. Worauf sich juristische Personen aber nicht mehr berufen können, sind die Betroffenenrechte wie etwa das Auskunftsrecht. Auch in den Datenschutzerklärungen müssen sie nicht mehr berücksichtigt werden (wohl aber ihre Mitarbeiter, wenn über diese Personendaten bearbeitet werden; sie sind als natürliche Personen weiterhin geschützt!).

Juristische Personen können sich in Bezug auf ihre Daten weiterhin auf das Gesetz gegen den unlauteren Wettbewerber (UWG) berufen und auch all jene Bestimmungen, die Geschäfts- und Berufsgeheimnisse schützen.

Ist in der Schweiz jetzt seitens EDÖB mit einer Bussenwelle zu rechnen?

Nein, davon ist nicht auszugehen. Der EDÖB darf gar keine Bussen verhängen, das dürfen nur die kantonalen Strafbehörden, und wie sehr diese DSG-Delikte verfolgen werden, wird sich zeigen. Es ist allerdings auch klar, dass von den Bussen nicht nur die oberen Kader betroffen sind, wie der Bundesrat dies vertrat, sondern jeder, der vorsätzlich an einer der mit Bussen bedrohten Verstössen teilnimmt. Das kann auch der Datenschutzbeauftragte sein, der mit Wissen und Willen eine falsche Auskunft erteilt oder vorsätzlich eine falsche Datenschutzerklärung aufschaltet. Die Tatbestände sind beschränkt (eine zu weitgehende Datenschutzbearbeitung genügt z.B. nicht); die DSGVO ist da viel strenger. Unter dem bisherigen DSG wurden so gut wie keine Bussen ausgesprochen, obwohl es sie teilweise schon gab.

Wahrscheinlicher ist, dass der EDÖB aktiv wird und durchaus nicht davor zurückschrecken wird, mit Verfügungen gegen nach seiner Ansicht renitente Unternehmen vorzugehen und beispielsweise Datenbearbeitungen direkt zu untersagen. Der Rechtsweg bleibt allerdings auch hier vorbehalten.

David Rosenthal

PS. Weitere Fragen von breiterem Interesse werden auf Wunsch gern aufgenommen.

[*] Die Inhalte dürfen in eigenen Unterlagen, Präsentationen, Schulungen, etc. verwendet werden; Nicht-Mitglieder bzw. Drittpersonen ausserhalb des VUD haben die Quelle anzugeben. Die Ausführungen stellen die Meinung des Autors dar, erfolgen ohne Gewähr, ersetzen nicht eine Rechtsberatung im Einzelfall und sind nicht als offizielle Position des VUD oder seiner Mitglieder zu verstehen.