VISCHER

Revision DSG

Update Entwurf Verordnung zum DSG (E-VDSG)

David Rosenthal
8. September 2021

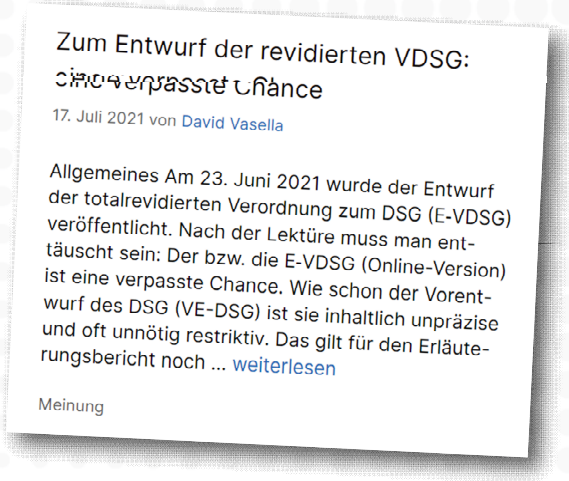
Wo stehen wir?

- **Vernehmlassung** zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)
  - Entwurf vom 23. Juni 2021, mit "erläuterndem Bericht"
  - Vernehmlassungsfrist bis **14. Oktober 2021**
- VDSG soll zeitgleich mit dem revidierten DSG in Kraft treten
  - Offiziell "in der zweiten Jahreshälfte 2022"
  - EDÖB: 1. Januar 2023

"Zahlreiche Bestimmungen im nDSG müssen auf Verordnungsebene konkretisiert werden. Bevor das Gesetz in Kraft treten kann, sind deshalb die entsprechenden Ausführungsbestimmungen in der VDSG grundlegend anzupassen." (Medienmitteilung)

Was wurde gemacht?

- Bereits innerhalb der Verwaltung sehr **umstrittene Vorlage**
- Ein Entwurf in Anlehnung an die bisherige VDSG, aber mit
  - Groben **Fehlern**
  - **Alten Zöpfen**, die abgeschnitten gehören
  - **Praxisfremden** Regelungen
  - Zahlreichen Bestimmungen **ohne Rechtsgrundlage**
- Erläuterungsbericht mit vielen **fachlichen Fehlern**
- Was tun? **Zurück an Absender** oder zahlreiche Bestimmungen streichen und anpassen


Zum Entwurf der revidierten VDSG: eine verpasste Chance

17. Juli 2021 von David Vasella

Allgemeines Am 23. Juni 2021 wurde der Entwurf der totalrevidierten Verordnung zum DSG (E-VDSG) veröffentlicht. Nach der Lektüre muss man enttäuscht sein: Der bzw. die E-VDSG (Online-Version) ist eine verpasste Chance. Wie schon der Vorentwurf des DSG (VE-DSG) ist sie inhaltlich unpräzise und oft unnötig restriktiv. Das gilt für den Erläuterungsbericht noch ... weiterlesen

Meinung

Was darf ein Verordnungsgeber?

BGE 141 II 169, E. 3.3:

«Die Kompetenz zum Erlass gesetzesvertretender Verordnungen setzt eine entsprechende Delegationsnorm im Gesetz voraus (Art. 164 Abs. 2 BV). Auch wenn der Gesetzgeber davon abgesehen hat, der Exekutive derartige (beschränkte) Legislativfunktionen zu übertragen, obliegt es dem Bundesrat, die Gesetzgebung zu vollziehen (Art. 182 Abs. 2 BV). Der Anwendungsbereich von Ausführungs- und Vollziehungsverordnungen ist indes darauf beschränkt, die Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher auszuführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Ausgangspunkt sind Sinn und Zweck des Gesetzes; sie kommen in grundsätzlicher Weise durch die Bestimmung im formellen Gesetz zum Ausdruck.»

Thema "Datensicherheit"

- Strafbar ist, wer vorsätzlich die "**Mindestanforderungen** an die Datensicherheit" nicht einhält, die der Bundesrat nach Art. 8 Abs. 3 erlassen hat
- Datensicherheit = Vertraulichkeit, Integrität und Verfügbarkeit
- Datensicherheit ≠ Bearbeitungsgrundsätze, Betroffenenrechte
- **E-VDSG** sieht dazu vor
  - Grundsätze
  - Schutzziele
  - Protokollierung
  - Bearbeitungsreglement

Datensicherheit: Grundsätze

Anpassen

- Datensicherheit darf **risikobasiert** erfolgen
- Wie kann eine Gesetzesnorm dem gerecht werden, gleichzeitig "Mindestanforderungen" definieren und trotzdem **bestimmt genug sein**, um Art. 1 StGB zu genügen?
- Die definierten Grundsätze tun es jedenfalls **nicht**
  - Legen Kriterien zur Beurteilung der Angemessenheit fest (z.B. Zweck, Art, Umfang der Datenbearbeitung, Stand der Technik, Risiko, Implementierungskosten)
  - Bisherige Liste wurde etwas ausgebaut
  - Definition von Risiko verwechselt Ursache und Wirkung
  - Überprüfung in "angemessenen Abständen"

Datensicherheit: Schutzziele

Streichen

- Die bereits bekannte Liste von Schutzzielen (Zugangskontrolle, Datenträgerkontrolle, Speicherkontrolle etc.) wurde erweitert
- Veraltetes Konzept – Giesskannenprinzip
- Schutzziele müssen "erreicht" werden: 100 Prozent Schutz?
- Besser wäre das Konzept von Art. 32 Abs. 1 DSGVO, welche Bestimmungen mögliche Massnahmen erwähnt, aber nicht zwingend vorgibt und auch nicht abschliessend ist

Datensicherheit: Protokollierung

Streichen

- Pflicht zur Einführung eines **Audit-Trails** für Bearbeitungen mit "hohem Risiko" für die Persönlichkeit oder die Grundrechte
- **Hoher Aufwand**, massive Datenbearbeitung
  - Jeder Benutzer wird bei jedem Schritt überwacht
  - Audit Trails für zwei Jahre aufbewahren
  - Aufbewahrung in vom operativen System getrennten Systemen
  - Protokolle dürfen nur für Datenschutzzwecke benutzt werden
- **Rechtsgrundlage fehlt**, Swiss Finish
  - Hier geht es nicht um Datensicherheit, sondern Datenschutz
  - Bundesrat hat auf Einführung einer Dokumentationspflicht im revDSG – ausser beim Inventar – bewusst verzichtet

Datensicherheit: Bearbeitungsreglement

Streichen

- Pflicht zur Führung eines "Bearbeitungsreglements" wenn **"umfangreich" besonders schützenswerte Personendaten** bearbeitet werden oder ein Profiling mit hohem Risiko besteht
  - Mindestangaben werden definiert (z.B. "Massnahmen, die zur Datenminimierung getroffen wurden", "Angaben zur Herkunft der Personendaten und zur Art ihrer Beschaffung")
- **Hoher Aufwand**
  - Ein weiteres, separates Dokument, das zu unterhalten ist …
- **Rechtsgrundlage fehlt**, Swiss Finish
  - Hier geht es nicht um Datensicherheit, sondern Datenschutz
  - Bundesrat hat auf Einführung einer Dokumentationspflicht im revDSG – ausser beim Inventar – bewusst verzichtet

Thema "Auftragsbearbeitung"

Streichen

- "Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz **verantwortlich**."
  - Kausalhaftung? Art. 41 ff. OR genügen …
- "Er muss **sicherstellen**, dass die Daten **vertrags- oder gesetzesgemäss** bearbeitet werden."
  - Gesetzliche Gewährleistung? Pflicht zur Vertragsdurchsetzung?
- Pflicht, "**gleichwertigen Datenschutz** [zu] gewährleisten" wenn der Auftragsbearbeiter dem DSG nicht untersteht
  - Verhältnis zu Art. 16 f. revDSG? Kausalhaftung?
- **Rechtsgrundlage fehlt**, Swiss Finish

Thema "Bekanntgabe ins Ausland"

Überarbeiten

- Inhaltliche **Vorgaben für Datenschutzklauseln** zum Schutz von Personendaten in unsicheren Drittländern
  - Wie z.B. Einhaltung der Bearbeitungsgrundsätze, die Namen der Staaten der Empfänger, Rechte der betroffenen Personen, Anforderungen an die Aufbewahrung von Daten
  - Keine Unterscheidung nach Controller und Processor
  - Keine vertragliche Meldepflicht für Data Breaches
- Pflicht **"sicherzustellen"**, dass der Empfänger im Ausland diese Datenschutzklauseln auch **einhält**
  - Nicht erfüllbar; DSGVO kennt keine solche Regelung

Thema "Informationspflicht"

Überarbeiten bzw. streichen

- Informationspflicht soll **auch für Auftragsbearbeiter** gelten
- Praxisfremde Erläuterungen (z.B. Empfehlung, am Telefon den Link zur Datenschutzerklärung zu nennen)
- Keine Klarstellung, dass Datenschutzerklärung auf Website in der Regel genügt – im Gegenteil
- Datenschutzerklärung muss "präzis" sein – noch genauere Angaben über die Datenbeschaffungen?
- Piktogramme "müssen" **maschinenlesbar** sein, obwohl es keinen Standard gibt, sie freiwillig sind und sie einem anderen Zweck dienen
  - Keine gesetzliche Grundlage; Strafbarkeit möglich?

Thema "Mitteilungspflichten"

Streichen

- Bei der Bekanntgabe von Personendaten muss der Empfänger über **Aktualität, Zuverlässigkeit und Vollständigkeit** der bekanntgegebenen Daten informiert werden
  - Sogar ein Auftragsbearbeiter wird verpflichtet
  - Nicht praktikabel
  - (Noch immer) keine gesetzliche Grundlage; Swiss Finish
- Verantwortliche haben **Empfänger** "unverzüglich" über Berichtigung, Löschung oder Vernichtung sowie Einschränkung der Bearbeitung von Personendaten **zu informieren**
  - War im Entwurf des revDSG vorgesehen, wurde jedoch vom Parlament gestrichen
  - Keine gesetzliche Grundlage

Thema "Dokumentationspflichten"

Streichen

- **Datenschutzfolgenabschätzung** muss "schriftlich" erfolgen
  - Textform muss jedoch genügen
  - Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden
- **Meldungen der Verletzungen der Datensicherheit**
  - Keine De-Minimis-Regelung, dafür Unnötiges (z.B. Erlaubnis, schrittweise zu informieren, wenn es nicht anders geht)
  - Sie müssen für drei Jahre dokumentiert werden (nur die meldepflichtigen?) mit allen "zusammenhängenden Tatsachen"
- Dokumentationspflichten haben **keine gesetzliche Grundlage**
  - Aufbewahrungsfristen erscheinen zufällig …

Thema "Auskunftsrecht"

Überarbeiten bzw. streichen

- **Nutzlose Regelungen** (im Sinne von "wenn alle einverstanden sind, darf die Auskunft auch mündlich begehrt werden")
- Ungenügende **Fristenregelung** und zu tiefe Kostenbeteiligung
- Pflicht, die Auskunft so zu erteilen, dass **die nachfragende Person sie versteht**
  - Was muss z.B. dem Teilnehmer einer medizinischen Studie erklärt werden, der alle von ihm erhobenen Daten haben will?
  - Geht viel zu weit; DSG sieht den subjektiven Ansatz nicht vor
- **Dokumentation** der Gründe für Einschränkung der Auskunft muss beim Verantwortlichen für drei Jahre dokumentiert sein
  - Auch hier: Keine gesetzliche Grundlage

Thema "Datenschutzberater"

Überarbeiten

- **Fehlende Abstimmung** zwischen Gesetz und Verordnung
  - Pflichtenheft wurde nicht aus dem Gesetz übernommen, sondern der bisherigen Verordnung (im bisherigen DSG gab es nichts)
  - Braucht es wirklich eine Regelung in der VDSG?
  - Gesetz: Schulung, Beratung, Mitwirkung an der Compliance
  - E-VDSG: Prüfung (aller?) Bearbeitungen und Empfehlung von Korrekturen, wo die Datenschutzvorschriften verletzt werden
- Aufgaben sind als persönliche **gesetzliche Pflicht** formuliert
  - Welche **Haftungsfolgen** hat dies für ihn/sie?

Thema "Verzeichnis"

Klarstellen

- Bundesrat kann Ausnahme von der Inventarpflicht vorsehen bei Unternehmen mit weniger als 250 Mitarbeitern und "deren Datenbearbeitung ein **geringes Risiko**" mit sich bringt
- Ausnahme soll dann nicht gelten, wenn ein "Profiling mit hohem Risiko" durchgeführt wird oder **umfangreich besonders schützenswerte Personendaten** bearbeitet werden
- Bedeutet dies im Umkehrschluss, dass nur diese beiden Fälle ein hohes Risiko mit sich bringen? Gilt dieser Massstab auch bei der Frage, wann es eine Datenschutz-Folgenabschätzung braucht?
- Ist die Ausnahme bei einer Datenbearbeitung nicht erfüllt, muss dann das Inventar für alle Aktivitäten gemacht werden?

Das bringt uns zur Schlussfrage:

Wie weiter?

VISCHER

Danke für Ihre Aufmerksamkeit!

Fragen: drosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com