VISCHER

Das neue DSG:

Was wir anders (und besser) machen können als die DSGVO

David Rosenthal
16. März 2021

Schweiz droht in der Datenökonomie ins Hintertreffen zu geraten

Der jüngste Bericht des Eidgenössischen Datenschutzbeauftragten mahnt zur beschleunigten Revision des Schweizer Datenschutzgesetzes. Und der Industrieverband Swissholdings sieht Schweizer Firmen benachteiligt, falls die EU die Gleichwertigkeit der inländischen Regulierung nicht mehr anerkennt.

Giorgio V. Müller
18.06.2019, 14.47 Uhr

Hören Merken Drucken Teilen

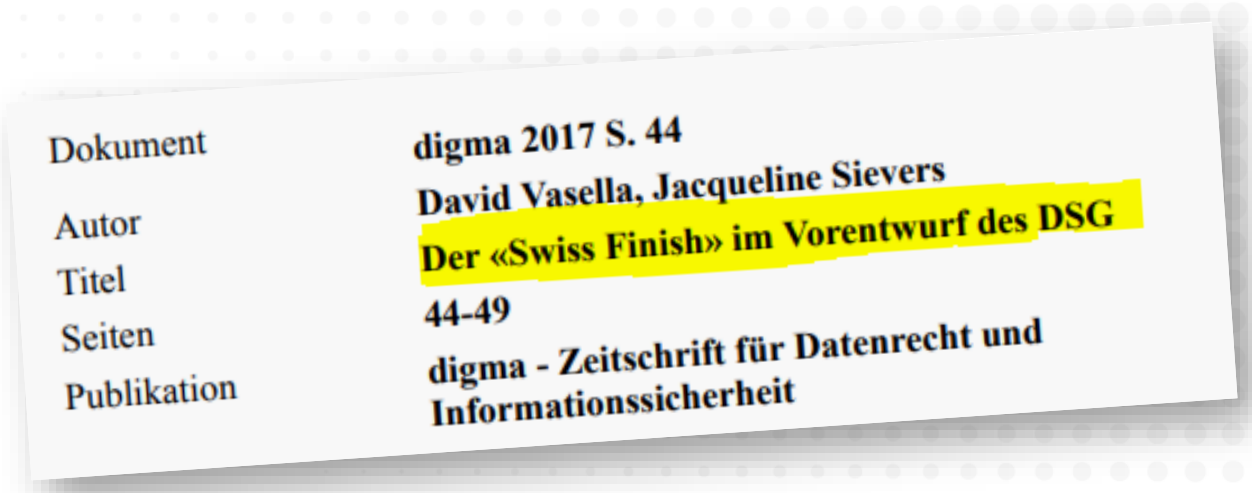
DSGVO einfach als solche übernehmen?

Quelle: www.nzz.ch

Gut Ding will Weile haben …

- Parlament benötigte **drei Jahre für die Totalrevision** des Datenschutzgesetzes (**DSG**)
  - Inklusive (unnötige) sechs Monate Diskussion um das "Profiling"
  - Inkrafttreten erst im Jahre 2022
- Haben wir eine **Kopie der DSGVO** erhalten? **Nein!**
- So wollte es das Parlament* – das DSG soll …
  - sich an die DSGVO "annähern", mit der DSGVO "vereinbar" und "äquivalent" sein, "sehr nahe an der DSGVO" liegen
  - aber nicht zur einer "Übernahme der DSGVO" führen
- Es **weicht** in etlichen Punkten davon **ab** – zum Glück!

* Fundstellen: BR Keller-Sutter, AB 2019 N 1782, 18. Dezember 2019; SR Fässler, 18. Dezember 2019, NR Glättli, AB 2019 N 1814; NR Romano, AB 2019 N 1778; NR Jauslin, AB 2019 N 1775; NR Wermuth, AB 2019 N 1777



Dokument	digma 2017 S. 44
Autor	David Vasella, Jacqueline Sievers
Titel	Der «Swiss Finish» im Vorentwurf des DSG
Seiten	44-49
Publikation	digma - Zeitschrift für Datenrecht und Informationssicherheit

Also weiterhin ein Swiss Finish?

Wo das neue DSG weiter geht

Gut für die Berater in der Schweiz!

- Sachlicher und räumlicher **Geltungsbereich** (Art. 2, 3)
  - Fast jede manuelle Datenbearbeitung wird erfasst
- Begriff der besonders schützenswerten Personendaten (Art. 5)
  - Verwaltungsrechtliche und strafrechtliche Verfolgung/Sanktionen
- **Informationspflichten** (Art. 19)
  - Generalklausel, Angabe der Staaten, in welche Daten exportiert werden und der Rechtsgrundlagen (bei unsicheren Drittstaaten)
- **Auskunftsrecht** (Art. 25 ff.)
  - Generalklausel und weniger Ausnahmen (Geschäftsgeheimnisse)
- **Persönliche Strafbarkeit**, kleines Berufsgeheimnis (Art. 60 ff.)

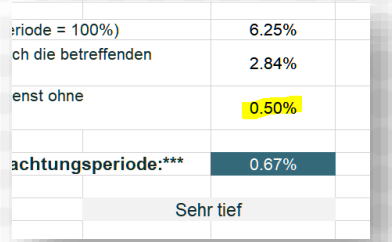
Wo wir es besser machen (können) als die EU

1. Bei der Bekanntgabe von **Personendaten ins Ausland** – weil ihr Umgang mit "Schrems II" ein Trauerspiel ist
2. In der Regulierung der **Einwilligung** – weil sie von der DSGVO und den Datenschutzbehörden kaputtgemacht wurde
3. Bei der **Informationspflicht** – weil sie eine Erfindung aus dem Elfenbeinturm ist
4. Mit der Pflicht zum **Privacy by Design** – weil es Drachentöter nur im Märchen gibt
5. Mit der Meldepflicht von **Data Breaches** – weil Behörden ihre Ressourcen für sinnvollere Dinge einsetzen sollten
6. Bei den **Sanktionen** für Datenschutzverletzungen – weil der Übermut der Datenschutzbehörden nicht zielführend ist

Personendaten ins Ausland

- Datenübermittlungen in die USA sollen nach Aussagen der Datenschützer verboten sein, wenn US-Nachrichtendienste ohne Gerichtsbeschluss auf Daten im Klartext zugreifen könnten
  - Der EuGH sagt dies in "Schrems II" zwar nicht so, aber der EDSA vertritt (bisher) einen Null-Risiko-Ansatz
  - Grund: Überforderung und Planlosigkeit
- Was tut der EDÖB? Er muss der EU nach dem Mund reden
  - Grund: Realpolitik, da Schweiz noch unter Beobachtung ist …
- Welche Massnahmen sind realistischerweise möglich?
- Welches Risiko ist akzeptabel? 50% in 691 Jahren?
- **Darum:** Zeigen wir der EU, was der risikobasierte Ansatz ist!

https://bit.ly/3ku4mOV



https://bit.ly/3dQA8Ep

nicht "perfekter" ...

Art. 16 Grundsätze

[1] Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.

[2] Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, so dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch:

a. einen völkerrechtlichen Vertrag;

b. Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner, die dem EDÖB vorgängig mitgeteilt wurden;

c. spezifische Garantien, die das zuständige Bundesorgan erarbeitet und dem EDÖB vorgängig mitgeteilt hat;

d. Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat; oder

e. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig

Nein! Dieses System wurde im Wissen um alle Unzulänglichkeiten vom Parlament so beschlossen

Einwilligungen

Abo Internetrichtlinien sorgen für Ärger

Selbst der Datenschützer nervt sich über Cookie-Warnungen

Wer im Internet surft, stösst ständig auf lästige Datenschutz-Richtlinien, die weggeklickt werden müssen. Eine Plage, die immer mühsamer wird.

Rico Bandle
Aktualisiert: 04.10.2020, 12:29
6 Kommentare

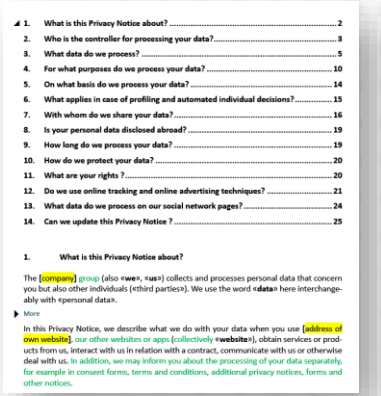
SonntagsZeitung, 4.10.2020

- Schon mal über Cookie-Banner geärgert?
- EU: Einwilligung als Schlüssel zur Sicherstellung der informationellen Selbstbestimmung
  - Anforderungen der DSGVO sind so hoch, dass Einwilligungen oft kein tauglicher Rechtsgrund mehr sind → "ABC"-Prinzip
- Schweiz: Keine erhöhten Anforderungen an Einwilligungen
  - Kein (strenges) Koppelungsverbot (BVerwG A-3548/2018)
  - Einwilligungen können verbindlich sein (BGE 136 III 401)
  - Vorangekreuzte Kästchen auf Formularen erlaubt (Art. 1 OR)
- Zudem: Bearbeitung von Daten erfordern keinen Rechtsgrund
- **Darum:** Lasst uns an unseren bewährten Regeln festhalten!

Informationspflichten

"Transparenzgrundsatz"
(bisher)

- Sind Datenschutzerklärungen (DSE) weniger spannend als die Zusammensetzung von Lebensmitteln?
  - Warum liest sie dann keiner? Weil sie zu lang sind?
- Jede Datenbeschaffung im Betrieb muss abgedeckt sein
- Wie ausführlich formulieren?
- Was tun, um auch jene Personen auf eine DSE hinzuweisen, mit denen kein Online-Kontakt besteht?
- **Darum:** Jeder Datenschützer sollte eine DSE für eine grössere Firma selbst verfassen, bevor er irgendwelche Forderungen stellt!



1. What is this Privacy Notice about? 2
2. Who is the controller for processing your data? 3
3. What data do we process? 5
4. For what purposes do we process your data? 10
5. On what basis do we process your data? 14
6. What applies in case of profiling and automated individual decisions? 15
7. With whom do we share your data? 16
8. Is your personal data disclosed abroad? 19
9. How long do we process your data? 19
10. How do we protect your data? 20
11. What are your rights ? 20
12. Do we use online tracking and online advertising techniques? 21
13. What data do we process on our social network pages? 24
14. Can we update this Privacy Notice ? 25

1. What is this Privacy Notice about?

The [company] group (also «**we**», «**us**») collects and processes personal data that concern you but also other individuals («third parties»). We use the word «**data**» here interchangeably with «personal data».

More

In this Privacy Notice, we describe what we do with your data when you use [address of own website], our other websites or apps (collectively «**website**»), obtain services or products from us, interact with us in relation with a contract, communicate with us or otherwise deal with us. In addition, we may inform you about the processing of your data separately, for example in consent forms, terms and conditions, additional privacy notices, forms and other notices.

"Informationspflicht"
(neu)

Eine Lizenz zum Gelddrucken …

50 Millionen Euro Datenschutz-Strafe für Google in Frankreich

Bei der ersten grossen Strafe im Zusammenhang mit der EU-
Datenschutzgr
50 Millionen E
Datenschutzbe
2018 geltende

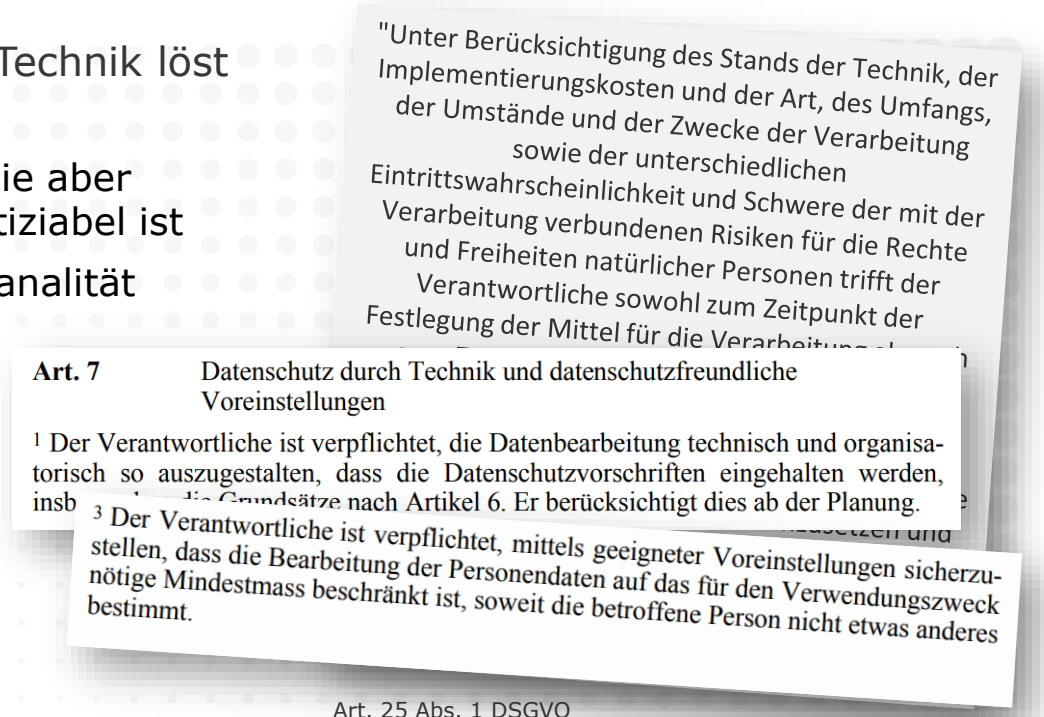
21.01.2019, 18.42 Uhr

Neue Zürcher Zeitung, 21.1.2019

(dpa) Wie die Behörde am Montag erklärte, seien unter anderem Informationen zur Verwendung der erhobenen Daten und dem Speicher-Zeitraum für die Nutzer nicht einfach genug zugänglich. Sie seien über mehrere Dokumente verteilt und Nutzer müssten sich über mehrere Links und Buttons durchklicken. Zudem seien einige der Informationen unklar formuliert.

Privacy by Design and Default

- Privacy by Design – die richtige Technik löst alle Datenschutzprobleme
  - Eine in der Theorie gute Idee, die aber weder massentauglich noch justiziabel ist
  - Gesetzgeber reduziert sie zur Banalität
- Privacy by Default – von der DSGVO übernommen und auf "Voreinstellungen" reduziert
  - Es zeichnet sich schon ab, dass die Klausel für andere Zwecke herhalten muss …
- **Darum:** Nichts hineindichten!



"Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung

Art. 7 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

[1] Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insb … die Grundsätze nach Artikel 6. Er berücksichtigt dies ab der Planung.

[3] Der Verantwortliche ist 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.

Art. 25 Abs. 1 DSGVO

Data Breach Notifications

- Haben Sie schon sichergestellt, dass bei falsch adressierten E-Mails etc. die neue Meldepflicht für Data Breaches eingehalten sein wird?
  - DSGVO: Bei jedem Risiko für betroffene Personen
  - DSG: Nur bei hohem Risiko für betroffene Personen
- Damit die Datenschutzbehörde prüfen kann, ob Sie auf die Verletzung der Datensicherheit richtig reagiert haben
  - Auch Meldefrist beim EDÖB und Pflicht zur Benachrichtigung betroffener Personen ist in der Schweiz vernünftiger geregelt
  - Trotzdem muss der EDÖB alles gründlich verarbeiten
- **Darum:** Wir sollten nur gewichtige Fälle melden müssen!

https://bit.ly/37TH0gm

Dänemark = 2/3 der Bevölkerung und 1/2 des BPI der Schweiz

27 Meldungen/Arbeitstag

VISCHER

Einbruch in Arztpraxis, wohl zur Beschaffung von Drogen, nicht den Patientenakten

Versicherungsagentur entsorgt Akten ständig ungeshreddert im offenen Abfall, Nachbar meldet es

Online-Shop gehackt, Passwörter gestohlen, nur einfach gehasht

Nicht besonders heikle E-Mail versehentlich an falschen, aber vertrauenswürdigen Empfänger

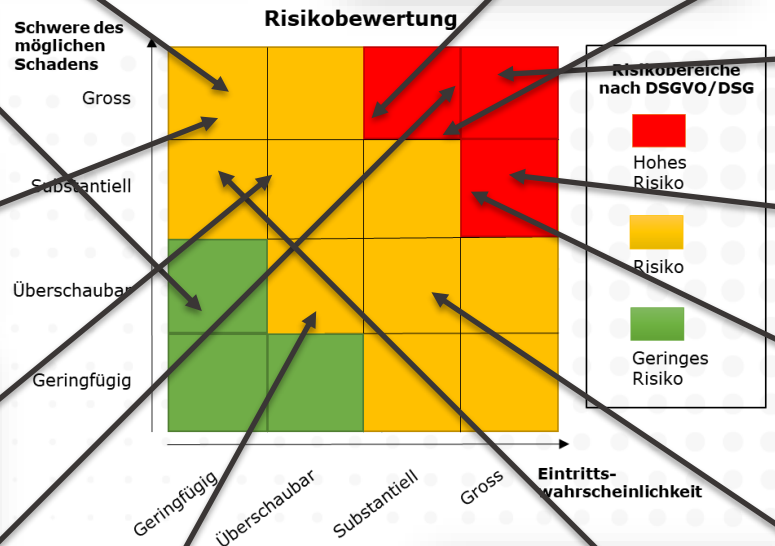
Mitarbeiter einer Bank entwendet Kundendaten

Firewall-Hersteller entdeckt alte Sicherheitslücke, die fremden Zugriff erlaubt, liefert Patch; kein Hinweis auf Zero-Day-Exploit

Professor verliert Prüfungsbögen, Prüfung muss wiederholt werden

Mitarbeiter unterhalten sich über heikle und vertrauliche Personalie im Zug für Dritte mithörbar, jedoch keine nützlichen Hinweise auf die Identität für Aussenstehende

Bank versendet aufgrund eines Fehlers hunderte Kontoauszüge natürlicher Personen an die falschen Kunden



Ausländische Strafbehörde beschlagnahmt Daten bei einem Cloud-Provider wider Schweizer Recht

Golf-Shop versendet Werbemail versehentlich mit offenen Empfängern

Mitarbeiter verliert USB-Stick mit unverschlüsselten Lohndaten, Stick taucht aber dank ehrlichem Finder rasch wieder auf

Online-Shop fällt temporär aus, kein Zugriff auf frühere Bestellungen

Sanktionen

"Fines and breach notifications continue their double digit annual growth and European regulators have shown their willingness to use their enforcement powers. They have also adopted some extremely strict interpretations of GDPR setting the scene for heated legal battles in the years ahead."
Ross McKean, DLA Piper

https://bit.ly/37TH0gm

- DSGVO: Behörden üben sich in strenger Auslegung, exzessiven Bussen – und in Verfahrensfehlern
  - Busse gegen 1&1 von EUR 9.55m auf 0.9m reduziert – ein rein umsatzorientiertes Bussgeldkonzept geht nicht*
  - Busse gegen Österreichische Post von EUR 18m aufgehoben – es fehlte die Angabe der verantwortlichen natürlichen Person**
  - Busse gegen Deutsche Wohnen von EUR 14.5m aufgehoben – "weil der Bussgeldbescheid unwirksam war"***
- Verbessern solche Bussen wirklich den Datenschutz?
- Schweiz: Bussen nur bei Vorsatz, nur für wenige Tatbestände und nicht vom EDÖB – aber dafür persönlich
- **Darum:** Nur als *ultima ratio* und mit Augenmass!

* Unzureichende Authentifizierung bei Anrufern im Call Center
** Unerlaubt politische Affinitäten ausgewertet und verkauft
*** Nicht mehr benötigte Daten wurden nicht gelöscht

Schlusswort

- Das neue DSG hält zum Glück an **bewährten Konzepten** fest
  - Beispiel: Bearbeitungen erfordern nicht per se einen Rechtsgrund
- Es deckt die DSGVO ab, fokussiert aber auf **Wesentliches**
  - Beispiel: Ein Widerspruchsrecht statt drei parallele Regelungen
- Trotzdem besteht noch **Grund zur Sorge** …
  - Es wird zu gern und unreflektiert von deutscher Lehre und Praxis abgeschrieben – so übernehmen wir auch ihre Übersteigerungen
  - Datenschutz ist besonders anfällig für "unintended consequences"
  - Der EDÖB verfolgt seine eigene Agenda
- **Darum:** Das DSG nicht einfach als Kopie der DSGVO behandeln!
  - Der Aufwärtskompatibilität zur DSGVO wird es nicht schaden

VISCHER

Ausführliche kostenlose Kommentierung: https://bit.ly/3kUfzqu

Danke für Ihre Aufmerksamkeit!

Bei 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