

VISCHER

Datenschutzrecht.

Eine kleine Einführung in die Praxis

David Rosenthal
23. August 2022

«Bezahlen oder Leiden» – das steckt hinter dem Hackerangriff auf Comparis.ch

Internet-Kriminelle haben den Schweizer Vergleichsdienst infiltriert,
Daten gestohlen und verschlüsselt. Die gleiche Gruppe zeichnet für den
ersten «Cyber-Katastrophenfall» Deutschlands verantwortlich.



© 15.07.2021, 17:25 ◻ 16.07.2021, 14:43

DARKTRACE Technologie Produkte Branchen Aktuelles Blog Infomaterial Unternehmen [Kostenlos testen](#)

Weltweit führend bei autonomer Cyber-KI

Das Darktrace Immune System ist die weltweit führende Plattform für eigenständige Cyberabwehr. Seine mehrfach ausgezeichnete **Cyber-KI** schützt Ihre Belegschaft und Ihre Daten vor raffinierten Angreifern, indem sie Cyberbedrohungen in Echtzeit erkennt, untersucht und abwehrt – egal wo der Angriff erfolgt.

[Entdecken Sie unsere Produkte >](#)

Überwacht den
ganzen
Datenverkehr im
Unternehmen
zwecks Abwehr
von Ransomware

Ist das erlaubt?

Unter welchen
Bedingungen?

1. Datenschutz vs. Datensicherheit

- Datensicherheit ist wichtig
- Datensicherheit ist aber nicht gleich Datenschutz
 - Nur ein Teilaspekt
- Datenschutz ...
 - schützt die Persönlichkeit vor Verletzungen in Folge der Bearbeitung von Personendaten
 - will angemessene informationelle Selbstbestimmung sicherstellen
- Darum gibt es
 - Regeln, wie Daten bearbeitet werden dürfen
 - Regeln, die die Befolgung der Regeln sicherstellen



DSG, DSGVO

2. Personendaten

- Datenschutz gilt nur für das Bearbeiten von Personendaten
- Personendaten = alle Angaben, die sich auf eine bestimmte oder eine bestimmbare Person beziehen
 - David Rosenthal?
 - 079 322 10 38?
 - Der Leiter des Datenschutzteams von VISCHER?
 - Der Benutzer, der sich am 23.8.2021 um 19:33 mit der IP-Adresse 122.31.90.34 in den Webserver eingeloggt hat?
 - Die Impfquote bei VISCHER ist 67.4 Prozent?
 - Immer eine Frage aus der Warte des Betrachters (welche Mittel er hat und ob er bereit ist, sie einzusetzen → BGE 136 II 508)
- Abgrenzen: Anonyme Daten, pseudonyme Daten, Sachdaten



VISCHER



Source: www.youtube.com

Sind das
Personendaten?

10-02-14 | FAST FEED

NYC Taxi Data Blunder Reveals Which Celebs Don't Tip—And Who Frequents Strip Clubs

By cross-referencing de-anonymized trip data with paparazzi photos, a privacy research could tell how much Bradley Cooper paid his driver.



[PHOTO: FLICKR USER PAULTOM2104]

In Brad Cooper's case, we now know that his cab took him to Greenwich Village, possibly to have dinner at Melibea, and that he paid \$10.50, with no recorded tip. Ironically, he got in the cab to escape the photographers! We also know that Jessica Alba got into her taxi outside her hotel, the Trump SoHo, and somewhat surprisingly also did not add a tip to her \$9 fare. Now while this information is relatively benign, particularly a year down the line, I have revealed information that was not previously in the public domain. Considering the speculative drivel that usually accompanies these photos (trust me, I know!), a celebrity journalist would be thrilled to learn this additional information.

Source: www.fastcompany.com [<https://bit.ly/3bssrB9>] (2014)

3. Grundsätze

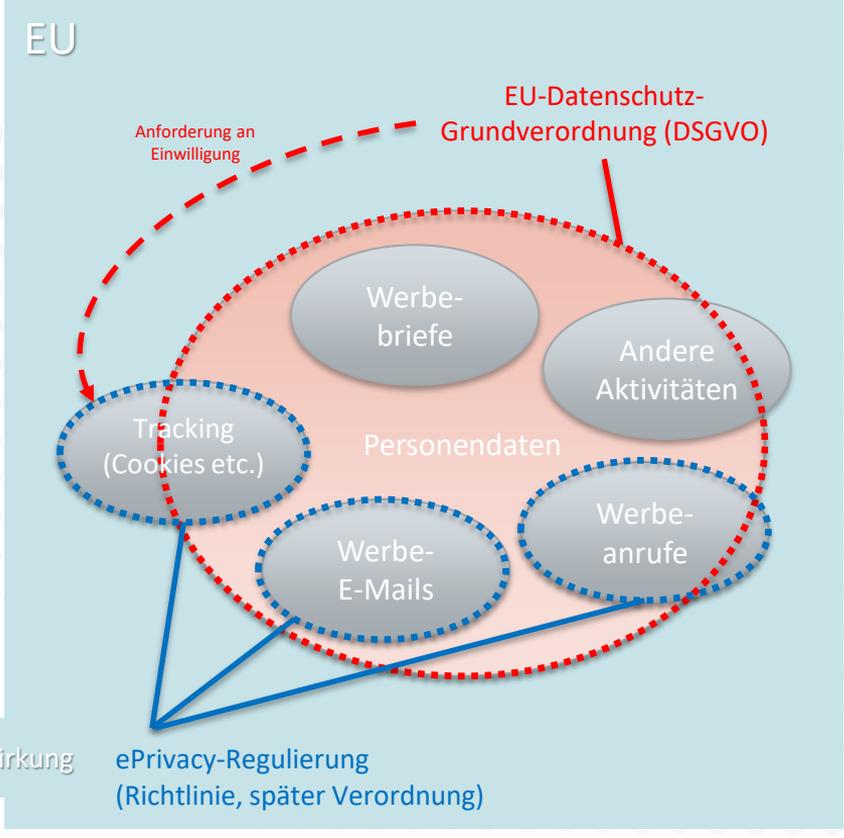
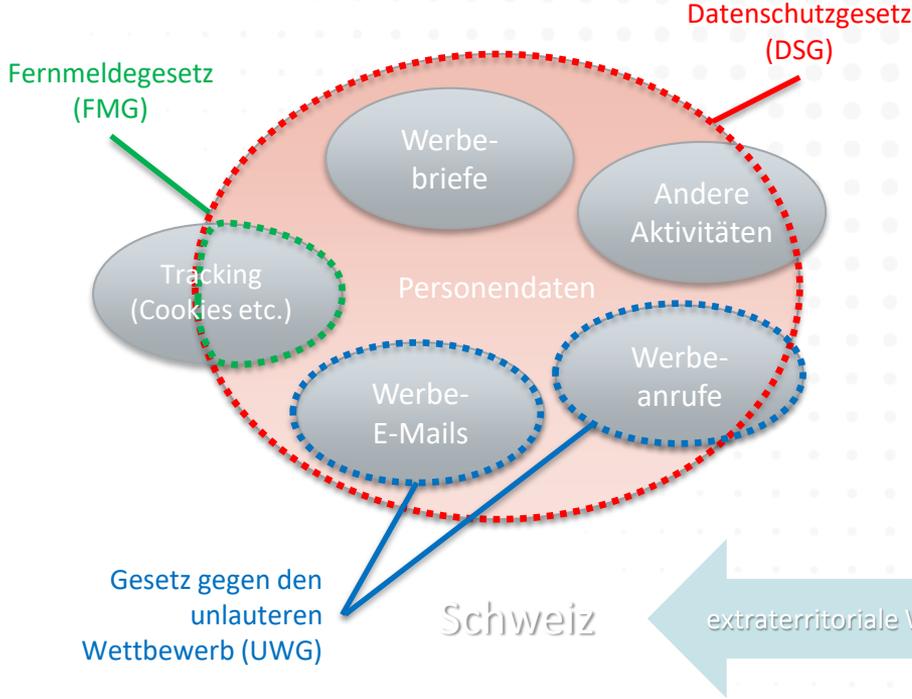
- Bearbeitungsgrundsätze
 - Transparenz
 - Zweckbindung (was kommuniziert wurde)
 - Verhältnismässigkeit (im Hinblick auf den Zweck)
 - Richtigkeit (im Hinblick auf den Zweck)
 - Datensicherheit, Treu und Glauben
- DSGVO: Es braucht immer einen Rechtsgrund (→ Art. 6, 9)
- DSG: Rechtfertigungsgrund nur, falls Bearbeitungsgrundsätze nicht eingehalten, der Betroffene widerspricht oder besonders schützenswerte Personendaten weitergegeben werden sollen
- Einwilligung, Vertrag, überwiegendes Interesse, Gesetz etc.

"ABC"-Prinzip
beachten!*

Privacy by Design

* Anything But Consent

4. Rechtsquellen

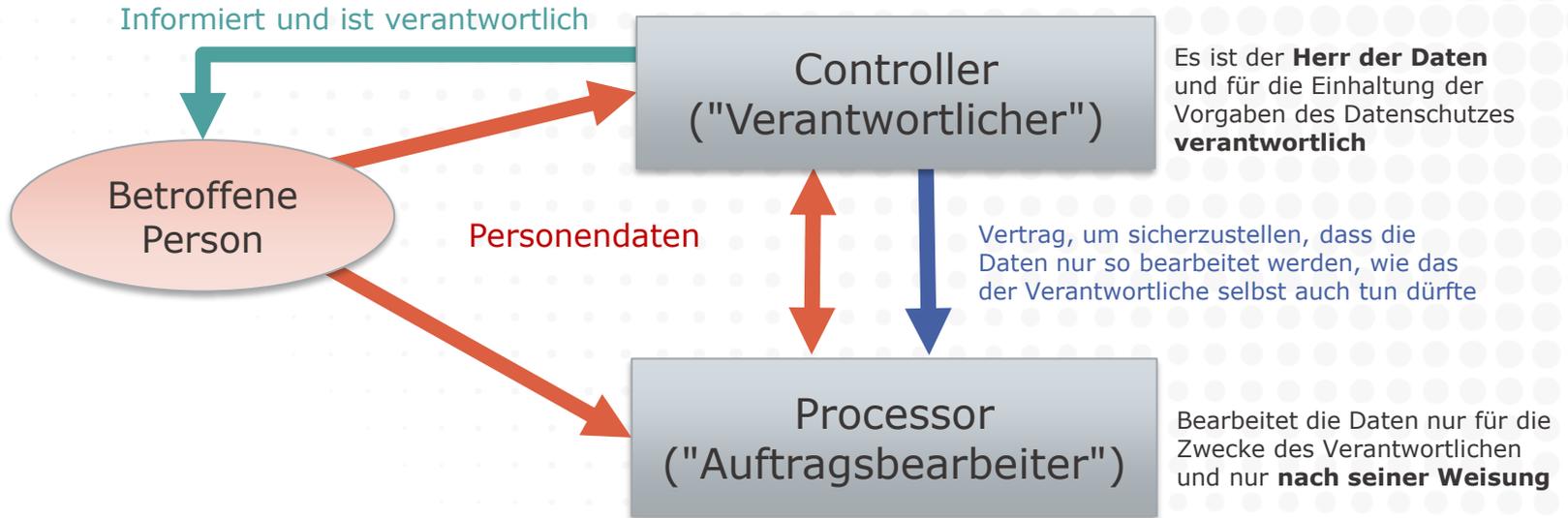


5. Örtlicher Geltungsbereich

Und VISCHER?

- DSGVO gilt ...
 - Für Betriebe im EWR
 - Für Betriebe ausserhalb des EWR, falls sie Privatpersonen ...
 - im EWR für ihre Waren oder Dienstleistungen dort gezielt anzusprechen versuchen
 - Im EWR mittels Internet oder anderer Technologien zu "tracken" oder sonst zu überwachen versuchen
 - Aber: Auf Nationalität kommt es nicht an
- Grossbritannien hat DSGVO übernommen ("UK GDPR")
- Schweizer DSG gilt – vereinfacht gesagt – bei jedem Schweizer Bezug (d.h. falls Handlung, Auswirkung, handelnde Person oder betroffene Person in der Schweiz)

6. Rollenverteilung





Pressemitteilung

Schriftarten sind nicht so banal, wie viele denken: Google Fonts löst Abmahnwelle aus

Erfurt, 18. August 2022: Aus aktuellem Anlass möchte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse über Folgendes informieren:

Drohende Abmahnwelle? Laut Medienquellen soll es aktuell zu einer Abmahnwelle gegen tausende von Websites-Betreibern kommen. Grund ist die dynamische Einbettung von Google Fonts auf deren Website, ohne vorab die Einwilligung der Besucher der Website einzuholen. Auch beim TLfDI gehen regelmäßig Beschwerden dieses Inhalts gegen Seitenbetreiber ein. Bei einer dynamischen Einbindung werden die Schriftarten von Servern des US-Konzerns in den Browser des Besuchers geladen und dabei personenbezogene Daten, wie z. B. die IP-Adresse der Benutzer, in die USA übermittelt.

Wo liegt hier das
datenschutzrechtliche
Problem?

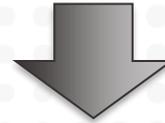


Max Schrems (noyb.eu)

By Manfred Werner - Tsui - Own work, CC BY-SA 3.0



Verklagte Facebook, weil diese Daten in die USA übermitteln, die dort von der NSA abgehört werden, was seine Grundrechte verletze

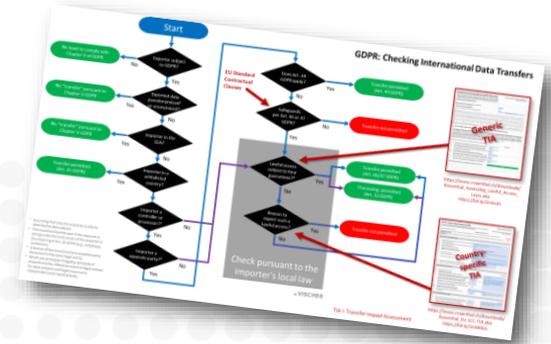
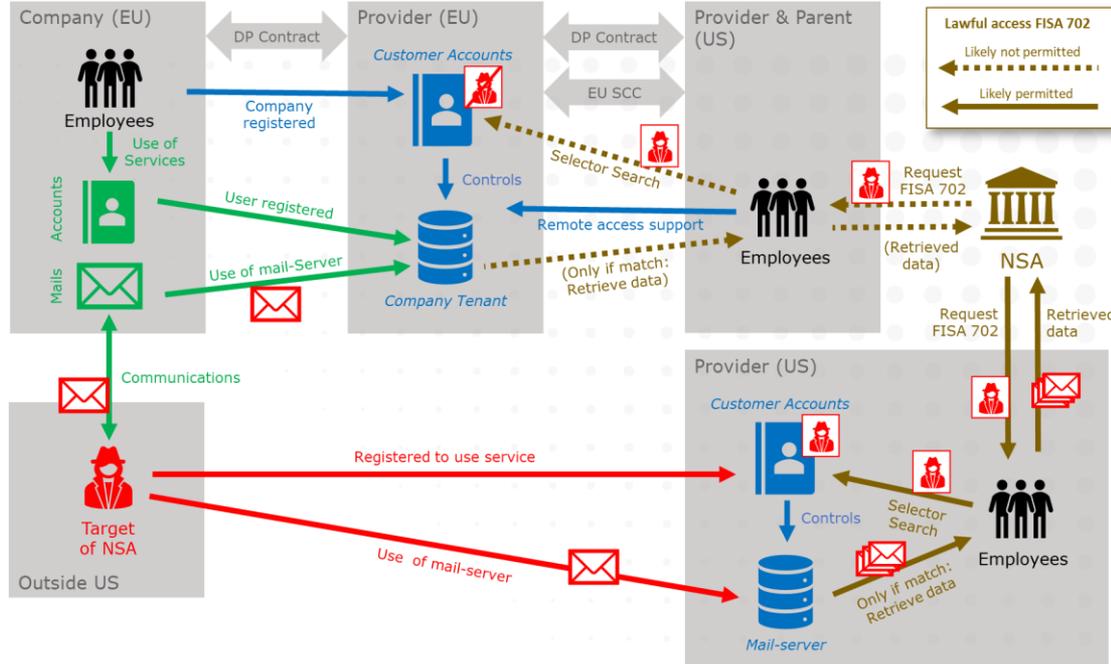


EuGH gab ihm am 16. Juli 2020 Recht (C-311/18, "Schrems II")

- Seither steht die Datenschutzwelt Kopf deswegen
- Wie gering muss das Abhörriisiko sein? Null? Theoretisch?
- EU-Datenschützer wollen Übermittlung von Personendaten (auch pseudonymisierte) in die USA verbieten
- EDÖB sympathisiert aus taktischen Gründen mit ihnen



VISCHER



https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx



<https://www.noties.consulting/grumpygdpr/>

<https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf>

7. Regeln zur Durchsetzung

- Verträge bei Datenübermittlungen in unsichere Drittstaaten und Abklärung, welche Behördenzugriffe trotzdem möglich sind
- Vertrag zwischen Verantwortlichen und Auftragsbearbeitern
- Verzeichnis der Bearbeitungsaktivitäten
- Datenschutzerklärung (→ Art. 13/14 DSGVO, Art. 19 revDSG)
- Datenschutzfolgenabschätzungen
- Meldepflicht bei Verletzungen der Datensicherheit
- Anspruch auf "menschliches Gehör" bei wichtigen, aber "nur" von einem Computer getroffenen Entscheiden
- Sanktionen (DSGVO: gegen Firma; revDSG: gegen Person)

8. Rechte der betroffenen Personen

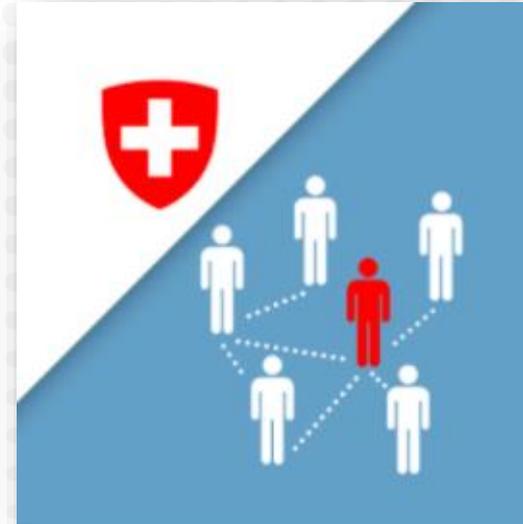
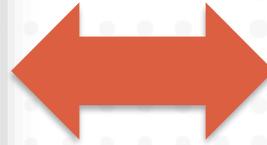
- Betroffene Personen können sie gegenüber Verantwortlichen (und teilweise Auftragsbearbeitern) geltend machen
- Auskunftsrecht
- Recht auf Datenportabilität
- Korrekturrecht
- Widerspruchsrecht
- Recht auf Löschung
- Widerruf einer Einwilligung
- Anspruch auf Schadenersatz und Unterlassung
- Möglichkeit der Beschwerde bei einer Datenschutzbehörde

9. Gefühlter Datenschutz

Bauchgefühl im Datenschutz:
<https://bit.ly/3moLiEH>



<http://petrafoede.de/blog/wp-content/uploads/2010/01/kaffeeklatsch-um-1900.jpg>



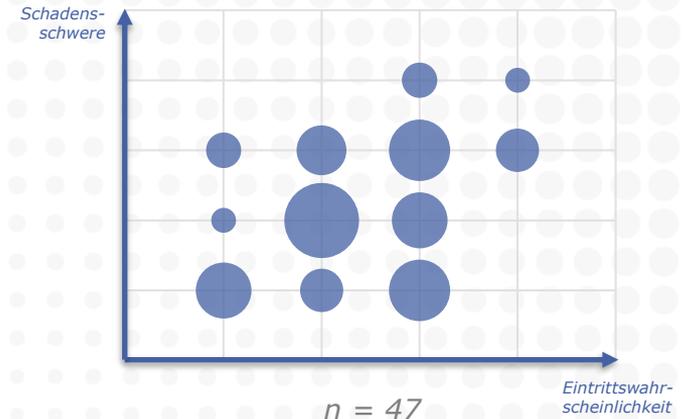
Das trügerische Bauchgefühl auch des Experten

"Eine Beraterfirma will ein Computerprogramm verwenden, das von jeder Stellenbewerbung eines Beraters einen "Erfolgsscore" aufgrund seines bisherigen Werdegangs und seiner Noten berechnet. Der Score basiert auf den bisherigen Erfahrungen des Unternehmens mit vergangenen Einstellungen. Der Score dient nur der Information des Hiring-Partners. Es wird niemand automatisch aussortiert."

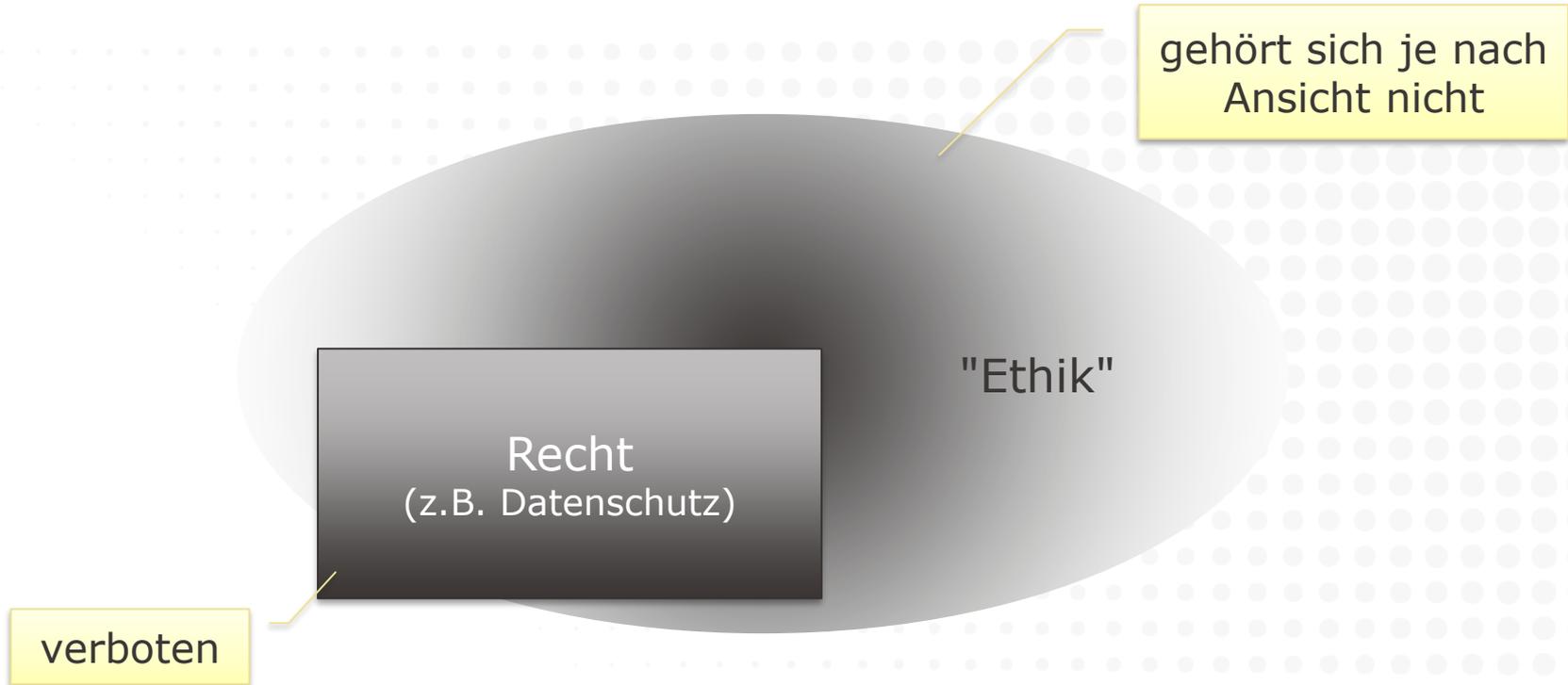
Was ist das Risiko für die betroffene Person?

<https://www.rosenthal.ch/downloads/Rosenthal-Beurteilung-Datenschutzrisiken.pdf>

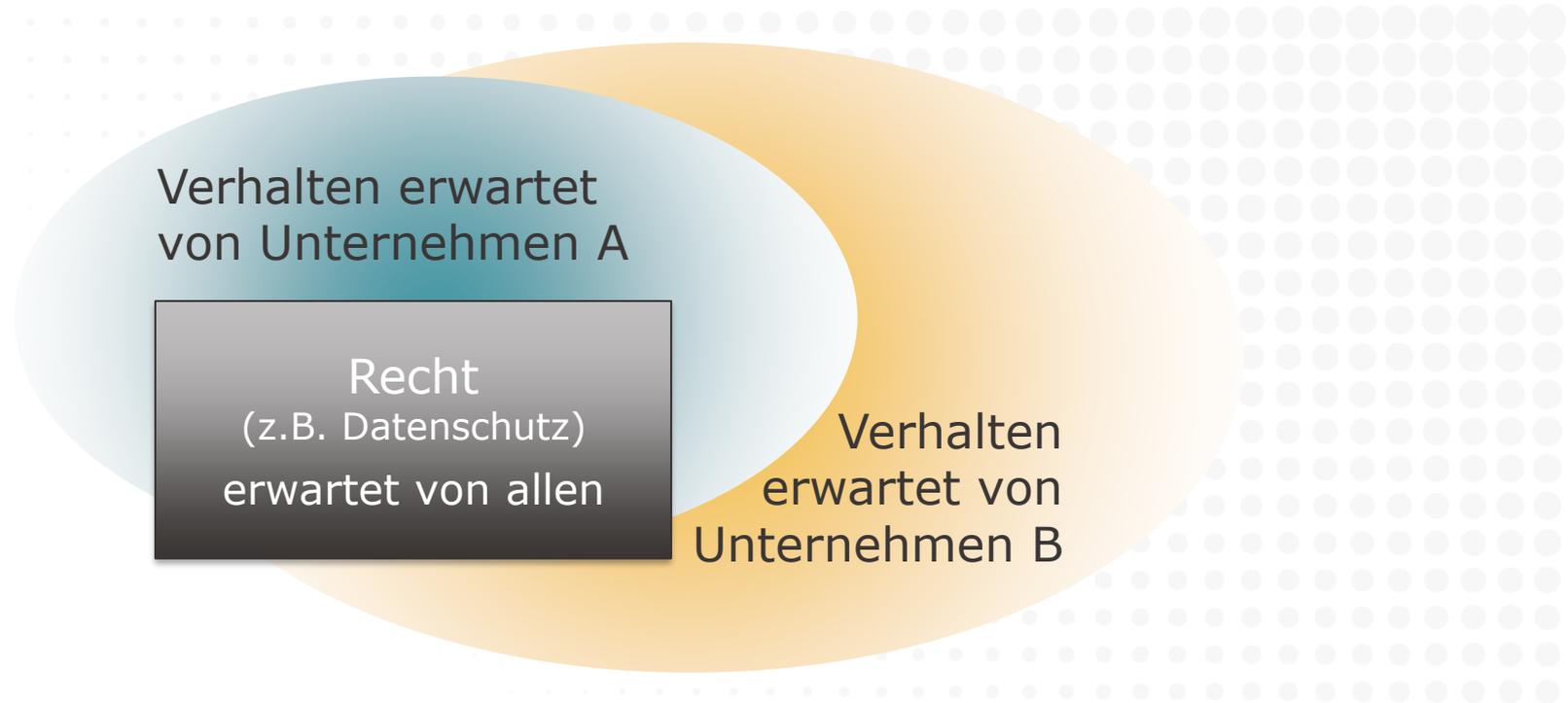
Ansichten von Datenschutz-Experten in einer Umfrage



Datenschutz vs. Datenethik



Realität ist also eher so ...



10. Aus der Praxis

- Niemand kann je vollständig datenschutzkonform sein
- Ohne risikobasierte Priorisierung und Entscheide geht es nicht
- Es gibt viele nicht wirklich qualifizierte "Datenschutzexperten" und daher tendenziell ein "race to the top"
- Noch immer sind viele Fragen ungeklärt
- Umsetzungsprojekte sind Herkulesprojekte, da Datenschutz jeden Bereich des Betrieb betrifft
- Hauptarbeit ist herauszufinden, was mit den Daten passiert
- Verantwortlich ist letztlich immer das "Business", nicht der betriebsinterne Datenschutzbeauftragte

Weiterführend zum neuen DSGVO

- Gesetzestext, mit Botschaft (verlinkt):
 - <https://datenrecht.ch/gesetzestexte/>
- Kostenlose Kommentierung (ca. 70 Seiten):
 - Deutsch: <https://bit.ly/3kUfzqu>,
 - Französisch: <https://bit.ly/3x9jrdU>
- Kompaktkurse in 60 Minuten: <https://bit.ly/3g5VnTa>
 - Zur Umsetzung des revidierten DSGVO
 - Zu den Unterschieden zur DSGVO
- Zu den Strafbestimmungen: <https://bit.ly/2SnxkGi>

Weitere Texte:
www.rosenthal.ch



VISCHER

Danke für Eure Aufmerksamkeit!

Fragen: drosenthal@vischer.com

Zürich

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

www.vischer.com

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