

VISCHER

Revision Datenschutzgesetz: Handlungsbedarf Marketing und Fundraising

David Rosenthal
24. Februar 2021

Ausgangslage

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

- Am 25. September 2020 verabschiedete das Parlament eine **Totalrevision des Datenschutzgesetzes** (DSG)
 - Text: <https://bit.ly/34PmN9h> (Vergleich: datenrecht.ch)
 - Jetzt folgen die Verordnungen, mit einer Vernehmlassung
 - Inkrafttreten erst in 2022, aber *ohne* Übergangsfrist
- Die Schweiz **schliesst im Datenschutz zur EU auf**
- Aber: Materiell **keine fundamentale Veränderung**
 - Bisher erlaubte Bearbeitungen sind i.d.R. weiterhin erlaubt
 - Keine Kopie der EU-Datenschutz-Grundverordnung (DSGVO), aber Diverses wird übernommen → <https://bit.ly/399bsEG>
 - Ausgebaut werden die Governance und Betroffenenrechte

Damit wir vom Selben reden ...

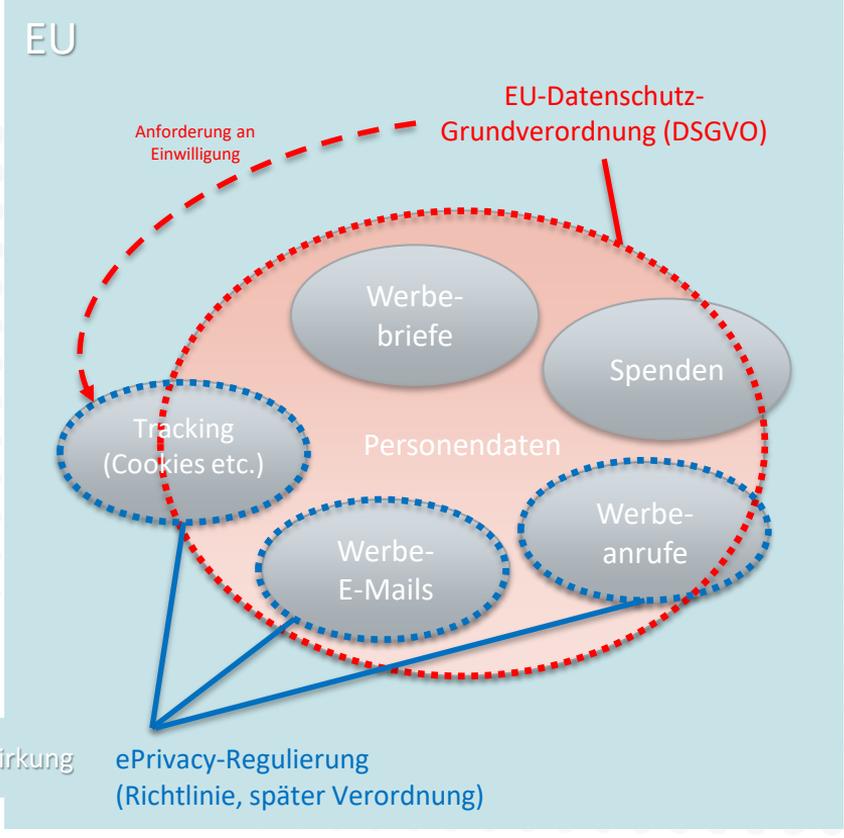
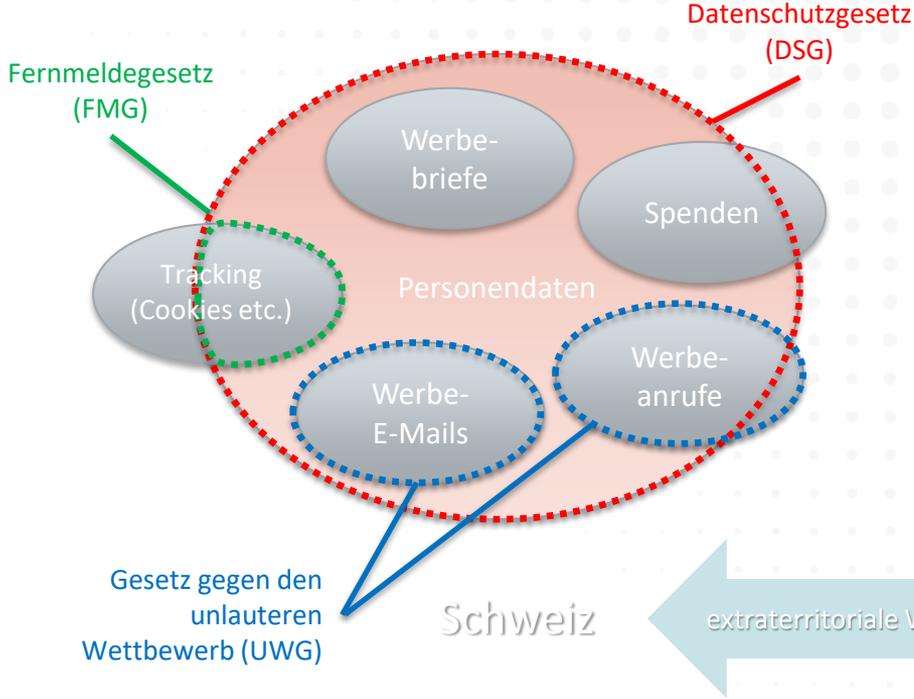
- **Personendaten** – nur Daten, die Rückschlüsse auf die Identität des Menschen erlauben, um den es geht
 - Das DSGVO gilt nur für den, der Personendaten bearbeitet
- **Besonders schützenswerte Personendaten** – bestimmte Arten von Personendaten (z.B. Gesundheitsdaten)
 - Das DSGVO sieht bei diesen leicht verschärfte Bestimmungen vor
- **Profiling** – ein Computer bewertet einen Menschen \neq **Profil**
 - Profiling als solches wird für die Privatwirtschaft kaum reguliert
- **Profiling mit hohem Risiko** – Profiling, welches zu einem Persönlichkeitsprofil (= diverse Aspekte eines Menschen) führt?
 - Einwilligungen müssen ausdrücklich sein, damit sie gültig sind

IP-Adressen
sind nach DSGVO
i.d.R. keine!
bit.ly/35TRzzC

z.B. autom.
Selektion von
Adressen nach
Affinität

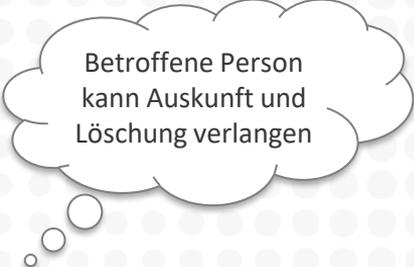
ausdrücklich =
beim Namen
genannt

Relevante Gesetze



Was Sie tun müssen

- Wenn Sie **Personendaten beschaffen**
 - Gegenüber betroffenen Person klarmachen, wozu Sie dies tun (= bisher) und auf Datenschutzerklärung hinweisen (= neu)
 - Nur Daten zwingend verlangen, die nötig sind (Rest optional)
 - Bei Adresseinkäufen Gewährleistung betr. Verwendungszweck verlangen (→ Vertrag, wie bisher)
- Wenn Sie **Personendaten bearbeiten**
 - Nur für jene Zwecke verwenden, die angegeben wurden
 - Stoppen, wenn jemand der Verwendung für Marketingzwecke widerspricht (→ Sperrliste) oder wenn Daten nicht mehr aktuell
- Wenn Sie ein **Mailing per Post** machen
 - Nur Daten verwenden, die korrekt beschafft wurden



Betroffene Person
kann Auskunft und
Löschung verlangen

Datenschutzerklärung

- **Informationspflicht**
 - Pflicht zur Datenschutzerklärung (DSE) für jede direkte und indirekte Datenbeschaffung (nicht nur Website-Nutzung)
- Gesetzlicher **Minimalinhalt** betreffend was geplant ist
 - Identität und Kontaktdaten des Verantwortlichen
 - Bearbeitungszweck
 - Kategorien von Empfängern (Dienstleister, Behörden etc.)
 - Beschaffte Daten (soweit aus Drittquellen)
 - Exportländer ("Europa") und Rechtsgrundlage für Exporte
- Weitergehende Angaben in **Ausnahmefällen**
- DSE muss mitgeteilt werden; **Hinweis mit Link** genügt i.d.R.

"Transparenzgrundsatz"
(bisher)



"Informationspflicht"
(neu)



Was Sie tun müssen

Weitere Ausführungen:
<https://bit.ly/3sbxYDa>

- Wenn Sie **Werbeanrufe machen** wollen
 - Anrufe nur mit einer erkennbaren Schweizer Rufnummer tätigen, die im Telefonverzeichnis eingetragen ist
 - Nur Nummern anrufen, die im Telefonverzeichnis ...
 - ohne "Stern" eingetragen sind oder
 - mit Stern oder gar nicht eingetragen sind, aber bei denen es eine aktuelle Geschäftsbeziehung (oder eine Einwilligung) gibt
 - Geschäftsbeziehung, damit der Werbeanruf nicht unerwartet ist
 - Werbeanrufe nur für gleichartige, eigene Angebote
 - Keine Anrufe an Personen, die keine Anrufe wollen (→ Sperrliste)
 - Keine telefonisch gewonnenen Informationen verwenden, wenn die Einhaltung dieser Regeln nicht sichergestellt worden ist

Prüfung vor
jedem Anruf

Beispiele

- Spendet jemand, nimmt er an einer Petition oder einem Event teil oder bestellt er eine Informationsbroschüre, so begründet dies eine Geschäftsbeziehung, womit Werbeanrufe trotz Stern oder nicht verzeichneter Telefonnummer für eigene, ähnlich Angebote möglich sind
- Liegt eine Spende oder ein Event ein Jahr zurück und gab es seither keine Transaktion, so darf die Person trotz Werbesperre noch angerufen werden; sind es drei Jahre ohne Kontakt, so ist die Geschäftsbeziehung wohl verfallen
- Spendet jemand per SMS, liegt eine Geschäftsbeziehung vor und sie kann trotz Werbesperre zu Werbezwecken angerufen werden

Was Sie tun müssen

Keine Änderung!

- Wenn Sie **Werbe-E-Mails senden** wollen
 - Erlaubter **Fall 1:**
 - Vertragsbeziehung besteht (z.B. aktueller Spender) und
 - Es wurde in der DSE oder Spendenformular auf Werbe-Mails und Abmeldemöglichkeit hingewiesen und
 - Werbung betrifft nur eigene ähnliche Angebote (z.B. Event)
 - Erlaubter **Fall 2:**
 - Person hat eingewilligt (z.B. DOI via Website, Wettbewerb, Einkauf von Adressen mit Opt-in, via AGB/Kleingedrucktes)
 - **In beiden Fällen:**
 - Korrekter Absender, einfache Abmeldemöglichkeit
 - Falls Tracking: Hinweis in der DSE nötig

Nicht für einzelne
E-Mails und Service-
Mails

Kästchen darf
vorangekreuzt
sein (nur CH)

Beispiele

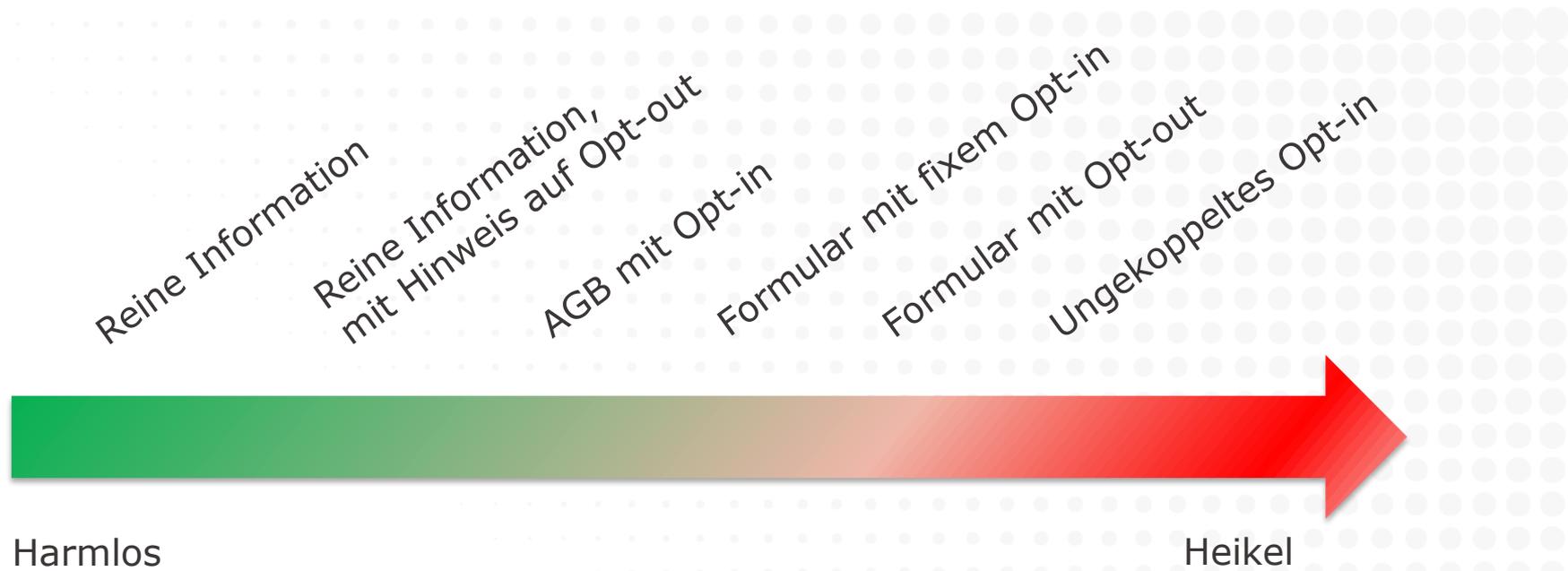
- Spendet jemand via Telefon, Internet oder auf der Strasse, wird er korrekt informiert und trifft die Spende ein, so begründet dies eine Vertragsbeziehung und er kann für Spenden oder für eigene Anlässe oder Initiativen per E-Mail beworben werden
- Willigt jemand in Erhalt von Werbung per E-Mail ein (ggf. mit Double-opt-in), so kann er bis zum Widerspruch angeschrieben werden (typisches Verfallsdatum: 2 Jahre ohne Interaktion); Einwilligung kann in der Schweiz mit anderem verknüpft sein
- Bestellt jemand etwas, darf dies auch Werbung enthalten; die Bestellung einer Infobroschüre führt jedoch weder zu einer Vertragsbeziehung noch zu einem Opt-in in Werbe-E-Mails
- Jemand empfiehlt einen Bekannten als Interessent: Einmaliges Anschreiben unter Hinweis auf die Quelle ist i.d.R. zulässig

Profilbildung erlaubt?

Kaum Änderung, aber
Praxis wird strenger

- Eine **Profilbildung** (\neq Profiling) für Werbezwecke kann mehr oder weniger weit gehen
 - Website-Tracking, Spenderprofil, Interaktionen, Social Media, etc.
 - Geht die Profilbildung besonders weit ...
 - ist ein besonderer Hinweis nötig (\rightarrow falls sie ungewöhnlich ist)
 - braucht es eine Einwilligung oder sonst ein überwiegendes Interesse (\rightarrow falls sie sonst als unverhältnismässig erscheint)
 - Widerspruch (d.h. Opt-out) bleibt so oder so möglich
- **Überwiegendes Interesse?** Speziell dort, wo die Profilbildung nicht personenbezogenen Zwecken dient (Erkenntnisgewinn)
- **Einwilligung?** Via AGB oder gesondert einholen ...

Je heikler, desto stärker Betroffene einbinden ...



Weitergabe an Dritte

- Eine Weitergabe an Dritte für deren Zwecke erfordert in der Regel eine **Einwilligung**, falls ...
 - sie nicht in der DSE oder sonst erwähnt war oder
 - sie als unverhältnismässig erscheint oder
 - es um besonders schützenswerte Personendaten geht
- Einwilligung kann i.d.R. jederzeit widerrufen werden
- **Information** in der DSE ist so oder so Pflicht
 - Kategorien von Empfängern (aber i.d.R. keine Namensnennung)
 - Nutzung von Daten für Werbezwecke Dritter erwähnen
- Anvertraute **geheime Daten**: Neues Berufsgeheimnis beachten

Kooperation mit Dritten

- Revidiertes DSGVO übernimmt Konzept vom "**Controller**" und "**Processor**" aus der DSGVO
 - Wer zusammen mit anderen den Zweck und die Mittel einer Datenbearbeitung bestimmt, ist gemeinsam verantwortlich
 - Beispiel: Eigene Website enthält Analyse- und Werbe-Tools von Dritten, welche die Daten auch für eigene Zwecke nutzen)
 - Gegenbeispiel: Cloud-Provider mit CRM-Lösung an (= Processor)
- Braucht es einen **Vertrag mit dem Dritten**?
 - Ja, im Falle eines Processors oder Exports in unsicheren Drittstaat
 - Im Falle eines gemeinsamen/selbständigen Controllers rechtlich nicht, aber eine Regelung der Datenverwendung wird empfohlen
- **Information** in der DSE über Kooperation mit den Dritten

Ausführlicher Beitrag zu Controller & Processor:
<https://bit.ly/3nPTawa>

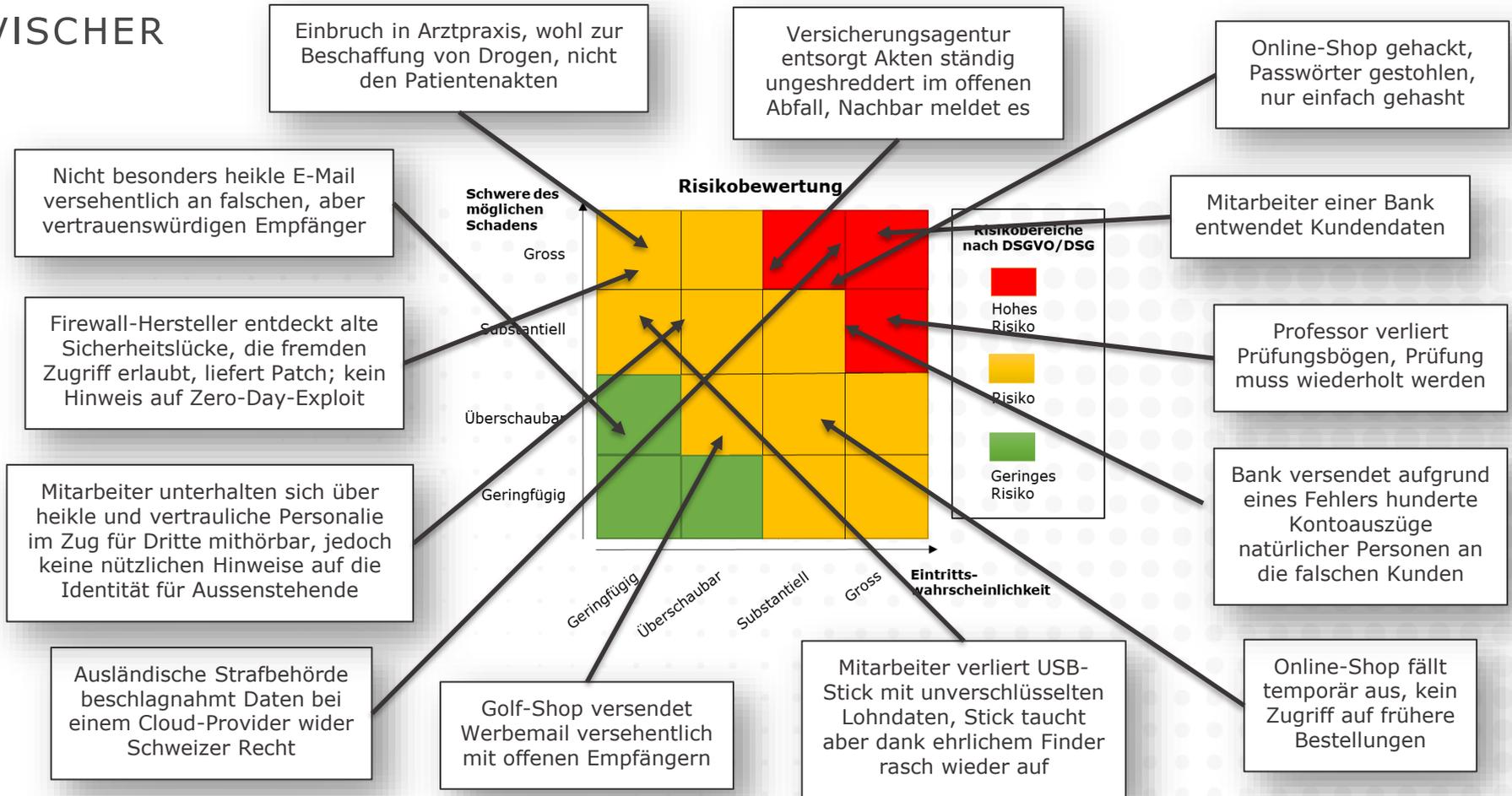
Google Analytics:
<https://bit.ly/2USiTrr>

Hier gibt es
Neuerungen

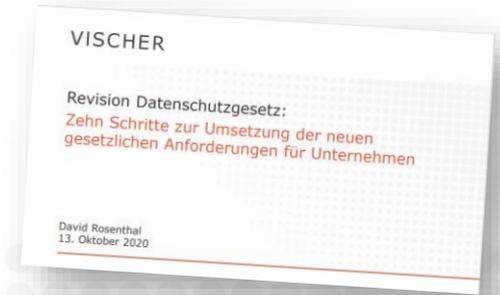
Neue Governance-Pflichten

- Pflicht zur Erstellung einer **Datenschutz-Folgenabschätzung**
 - Bei allen heiklen Datenbearbeitungs-Vorhaben
 - (Selbst-)Darstellung (i) der Datenbearbeitung und Massnahmen zum Datenschutz, (ii) der Risiken (d.h. Nachteile) für betroffene Person, (iii) etwaiger noch nötige Massnahmen, (iv) Beurteilung, ob ein "hohes" Risiko vorliegt (falls ja → Konsultation EDÖB)
- **Verzeichnis aller Datenbearbeitungen** des Unternehmens
- **Meldung von Verletzungen der Datensicherheit**
 - Unplanmässige Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von Daten (d.h. nicht jede Datenschutzverletzung)
 - Meldung an EDÖB falls "hohes Risiko" für betroffene Personen

VISCHER



Wie mit dem neuen DSGVO umgehen?



<https://bit.ly/2UTFXL6>

- Gibt es ein **Minimalprogramm**?
 - Inventar – keine Doktorarbeit machen (ein Excel genügt)
 - Datenschutzerklärung – weil sie Ihr Aushängeschild ist
 - Korrekte Verträge mit Dritten – weil Sie gebüsst werden können
 - **Aber:** Bussen werden die Ausnahme sein
- Was, wenn Sie intern **kein vertieftes Know-how** haben?
 - Bauen sie es intern auf – von aussen genügt i.d.R. ein Coaching
 - Sich vorbereiten auf: Anfragen von Betroffenen, Data Breaches
- Aktivitäten **risikobasiert** auf DSGVO-Compliance überprüfen
 - Ihre grössten Risiken sind (weiterhin) in Marketingaktivitäten
 - Praxis-Handbuch von Swissfundraising weiterhin eine gute Basis

Ergänzt durch den Jusletter-Beitrag und Beitrag über Telefonwerbung

VISCHER

Und nun zu Ihren 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
