VISCHER

Data Governance.

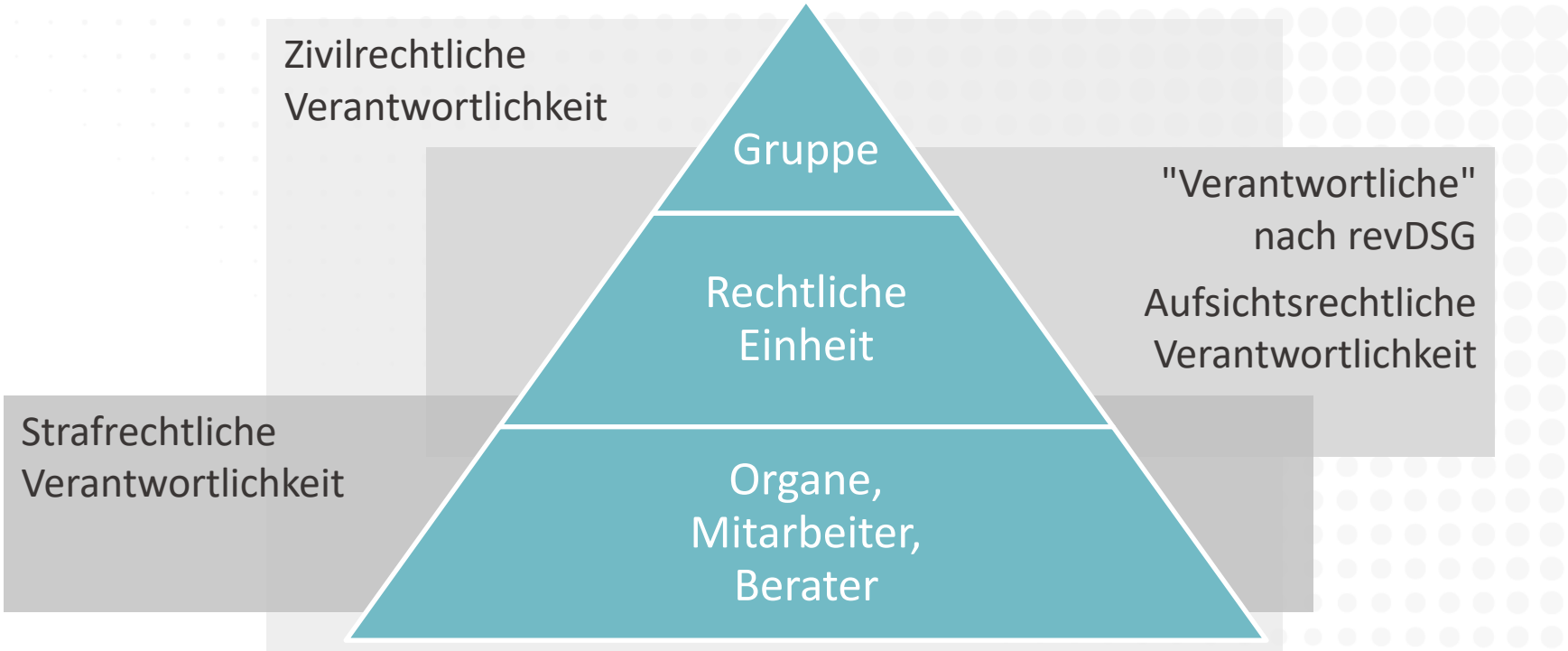
Wer ist für was verantwortlich?

David Rosenthal, Partner, VISCHER AG
24. Mai 2023

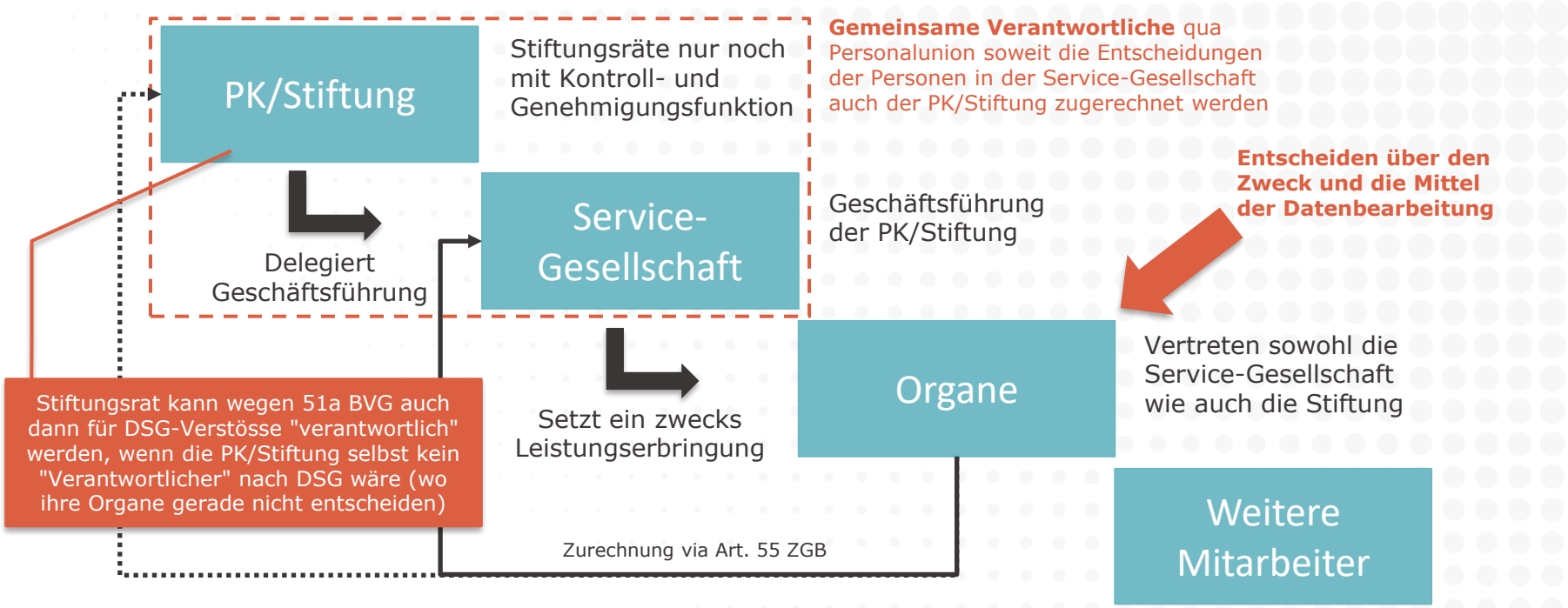
Verantwortlichkeit?

- **Zivilrechtliche Verantwortlichkeit**
  - Gegenüber betroffenen Personen
  - Gegenüber dem Arbeitgeber
  - Gegenüber Vertragspartnern (Provider, Kunden, Partner)
- **Aufsichtsrechtliche Verantwortlichkeit**
  - Durch den EDÖB
  - Durch andere Behörden (z.B. FINMA, BSV, BAG)
- **Strafrechtliche Verantwortlichkeit**
  - Aus revDSG
  - Aus anderen Normen (z.B. UWG)

Verantwortlichkeit?



"Verantwortliche" nach revDSG – Beispiel PK



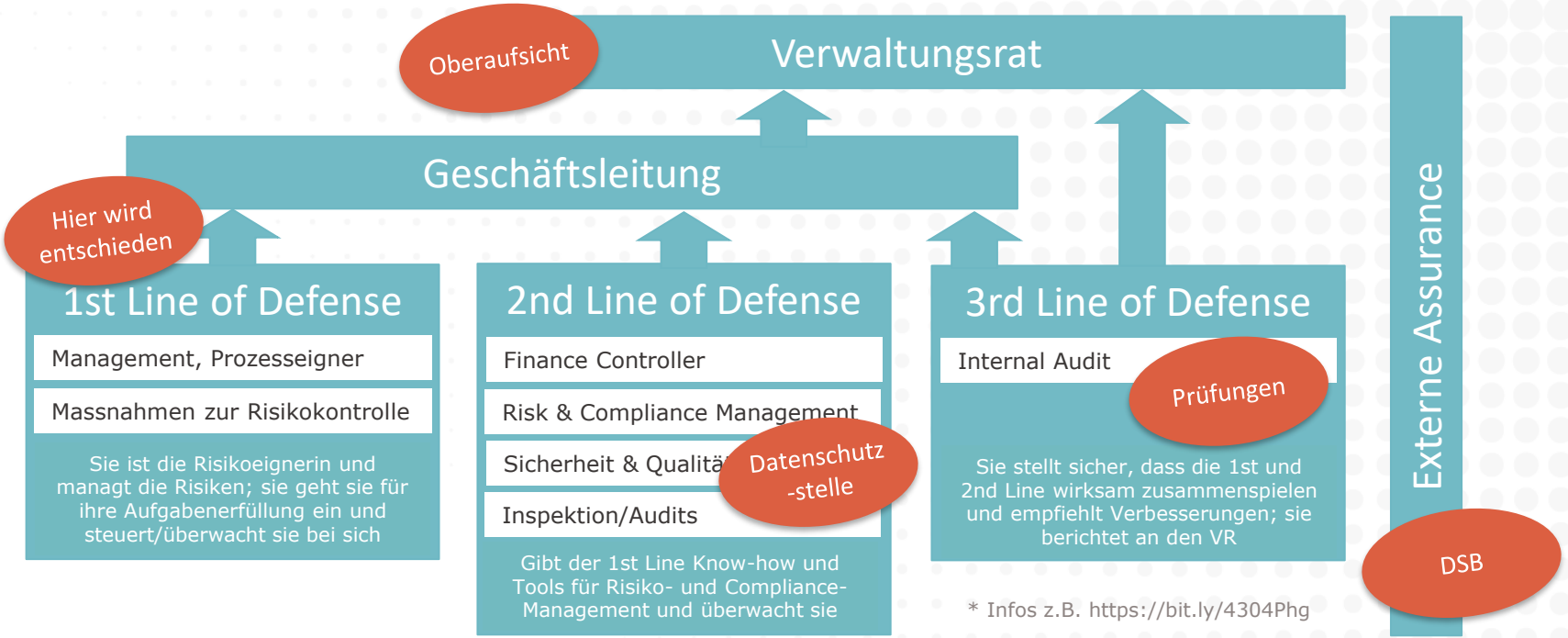
Wer ist intern verantwortlich?

- **Differenzieren** zwischen
  - Mit der weisungsgemässen Ausführung der Aufgabe betraut sein
  - Rechenschaftspflicht darüber, dass und wie sie ausgeführt wird
  - "Responsible" vs. "Accountable" im RACI-Modell*
- **Beispiel Bearbeitungsverzeichnis**
  - Die Datenschutzstelle führt es bei sich
  - Die Abteilungsleitungen sind für ihren Teil rechenschaftspflichtig und verantwortlich für die Meldung bei Anpassungsbedarf
- Es sollte möglichst **nur eine Person** rechenschaftspflichtig sein
- Sie trifft die wesentlichen **Entscheide**

* Infos z.B. https://asana.com/de/resources/raci-chart

Das "Three Lines of Defense"-Modell*

Seit 20 Jahren



* Infos z.B. https://bit.ly/4304Phg

Der "Datenschutzbeauftragte"

- **DSGVO** – Watchdog, Berater & Anlaufstelle, je nach Risikolage besteht eine Pflicht zur Bestellung
- **DSG** – Nur Berater und Anlaufstelle, keine Pflicht zur Bestellung (beides ausser bei Bundesorganen)

[2] Die Datenschutzberaterin oder der Datenschutzberater ist Anlaufstelle für die betroffenen Personen und für die Behörden, die in der Schweiz für den Datenschutz zuständig sind. Sie oder er hat namentlich folgende Aufgaben:

a. Schulung und Beratung des privaten Verantwortlichen in Fragen des Datenschutzes;

b. Mitwirkung bei der Anwendung der Datenschutzvorschriften.

Art. 10 revDSG
(Art. 26 DSV analog)

Sie oder er wirkt bei der Anwendung der Datenschutzvorschriften mit, indem sie oder er insbesondere:

1. die Bearbeitung von Personendaten prüft und Korrekturmassnahmen empfiehlt, wenn eine Verletzung der Datenschutzvorschriften festgestellt wird,
2. den Verantwortlichen bei der Erstellung der Datenschutz-Folgenabschätzung berät und deren Ausführung überprüft.

Art. 26 Abs. 2 DSV
(nur Bundesorgane)

Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

(a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

(b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

(c) Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;

(d) Zusammenarbeit mit der Aufsichtsbehörde;

(e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Art. 39 DSGVO

Der "Datenschutzbeauftragte"

AUTORITEIT PERSOONSGEGEVENS

NL | AND

Home About privacy Subjugate Do it yourself Publications Cont

Concerns about internal supervision of the municipality of Amsterdam

News release / 8 May 2023 Category: Municipalities

The Dutch Data Protection Authority (AP) has asked aldermen Van Buren (P&O) and Scholtes (ICT) to come to the DPA on behalf of the Board of B and W of the municipality of Amsterdam to explain the position of their internal privacy supervisor. The DPA is concerned about whether the independence of internal supervision at the municipality of Amsterdam is sufficiently regulated. Organisations are required by law to employ an internal privacy supervisor (the data protection officer, DPO) who independently supervises the organisation and provides advice to the organisation.

Hat wer ein Unternehmen in Datenschutzfragen berät oder für die Ausführung von Datenschutzarbeiten verantwortlich ist die nötige Unabhängigkeit?

Automatische Übersetzung von https://autoriteitpersoonsgegevens.nl/nl/nieuws/zorgen-over-intern-toezicht-gemeente-amsterdam

Der "Datenschutzberater"

- **Voraussetzungen** nach Art. 10 Abs. 3 revDSG, Art. 26 DSV
  - Fachlich unabhängig und weisungsungebunden
  - Keine Interessenkonflikte
  - Erforderliche Fachkenntnisse
  - Veröffentlichung Kontaktdaten und Mitteilung an EDÖB
- **Weitere Voraussetzungen** nach Art. 23 & 27 DSV
  - Notwendige Ressourcen (nur privater Sektor)
  - Zugangsrecht
  - Anspruch auf Meldung von Data Breaches (nur Bundesorgane)
  - Berichtsrecht an oberstes Leitungsorgan (nur privater Sektor)

Intern oder extern?

Darf er für Datenschutzprozesse verantwortlich sein?

Wo die Verantwortlichkeit beginnt

Art. 716*a*[579]

2. Unübertragbare Aufgaben

[1] Der Verwaltungsrat hat folgende unübertragbare und unentziehbare Aufgaben:

1. die Oberleitung der Gesellschaft und die Erteilung der nötigen Weisungen;
2. die Festlegung der Organisation;
3. die Ausgestaltung des Rechnungswesens, der Finanzkontrolle sowie der Finanzplanung, sofern diese für die Führung der Gesellschaft notwendig ist;
4. die Ernennung und Abberufung der mit der Geschäftsführung und der Vertretung betrauten Personen;
5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;
6. die Erstellung des Geschäftsberichtes[580] sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse;
7. [581] die Einreichung eines Gesuchs um Nachlassstundung und die

Obligationenrecht

Rollenverteilung

- **Verwaltungsrat**
  - Oberaufsicht über die Einhaltung des Datenschutz
  - Delegiert die Umsetzung an die GL
- **Geschäftsleitung**
  - Trifft die nötigen Massnahmen zur Umsetzung im Betrieb
  - Trifft die nötigen Entscheide zur Bearbeitung
- **Datenschutzstelle** ("Data Protection Compliance Officer")
  - Erarbeitung der Vorgaben, Beratung in deren Umsetzung, Überprüfung deren Umsetzung, Inhaber Datenschutzprozesse
- **Inhaber der Datenbearbeitungen** ("Data Activity Owner")
  - Treffen die nötigen Entscheide und sorgen für deren Umsetzung

In Grundsätzen regeln

In Datenschutz-weisung regeln

Der "Data Activity Owner" (DAO)

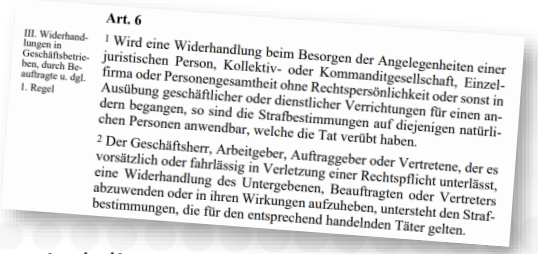
"Sofern die Geschäftsleitung im Einzelfall nichts anderes festgelegt hat, gilt der 'wirtschaftliche Berechtigte' der First Line of Defense als der DAO der betreffenden Bearbeitungsaktivität, d.h. der Business Owner jener Geschäftsaktivitäten, wo die Bearbeitung von Personendaten stattfindet und für welche die Bearbeitungsaktivität durchgeführt wird. Darüber hinaus gilt jede andere Person, welche die betreffende Bearbeitung ganz oder teilweise kontrolliert, als DAO; "Kontrolle" bedeutet die rechtliche oder faktische Befugnis, Entscheidungen über Aspekte der Bearbeitungsaktivität zu treffen oder das tatsächliche Treffen solcher Entscheide, jeweils sofern diese für die Einhaltung der Richtlinie oder des geltenden Datenschutzrechts wesentlich sind (z.B. die Kategorien der erhobenen Personendaten, die Kategorien der Empfänger von Personendaten, die Aufbewahrungsfristen). Gibt es mehrere DAO für dieselbe Tätigkeit, so ist jeder DAO für seine eigenen Entscheide und jene der ihm unterstellten DAO verantwortlich."

Quelle: Governance-Anhang der VISCHER Standard-Weisung für den Datenschutz

Entscheide?

- **Wer entscheidet …**
  - Wie Daten bearbeitet werden?
  - Welche Risiken werden eingegangen?
  - Welche Risiken in einer Datenschutz-Folgenabschätzung wie ausgewiesen werden?
  - Wie auf Begehren von Betroffenen reagiert wird?
  - Welche Auskunft erteilt wird?
  - Welche Data Breaches wem wie gemeldet werden?
- Die **Geschäftsleitung** bzw. der **"Data Activity Owner"**
  - **Nicht** die Datenschutzstelle! Sie berät nur, führt aus, überwacht
  - Dies sollte in der **Datenschutzweisung** festgehalten sein

Strafbarkeit



III. Widerhandlungen in Geschäftsbetrieben, durch Beauftragte u. dgl.
1. Regel

Art. 6

[1] Wird eine Widerhandlung beim Besorgen der Angelegenheiten einer juristischen Person, Kollektiv- oder Kommanditgesellschaft, Einzelfirma oder Personengesamtheit ohne Rechtspersönlichkeit oder sonst in Ausübung geschäftlicher oder dienstlicher Verrichtungen für einen andern begangen, so sind die Strafbestimmungen auf diejenigen natürlichen Personen anwendbar, welche die Tat verübt haben.

[2] Der Geschäftsherr, Arbeitgeber, Auftraggeber oder Vertretene, der es vorsätzlich oder fahrlässig in Verletzung einer Rechtspflicht unterlässt, eine Widerhandlung des Untergebenen, Beauftragten oder Vertreters abzuwenden oder in ihren Wirkungen aufzuheben, untersteht den Strafbestimmungen, die für den entsprechend handelnden Täter gelten.

VStrR

"Mit Busse bis zu 250'000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich …"

"Bei Widerhandlungen in Geschäftsbetrieben … sind die Strafbestimmungen auf diejenigen natürlichen Personen anwendbar …"

Strafrechtliche Verantwortlichkeit

- Auskunftsrecht
- Informationspflicht
- Pflicht zum AVV
- Bekanntgabe ins Ausland
- Datensicherheit
- Weisungen des EDÖB
- Berufsgeheimnis (tw.)

Durch Handeln

Jeder, der handelt

Beispiele:

- Wer in Kauf nimmt, eine falsche Auskunft an einen Betroffenen zu erteilen
- Wer entscheidet, die Datenschutz-Erklärung nicht wie erforderlich nachzuführen

Durch Unterlassen

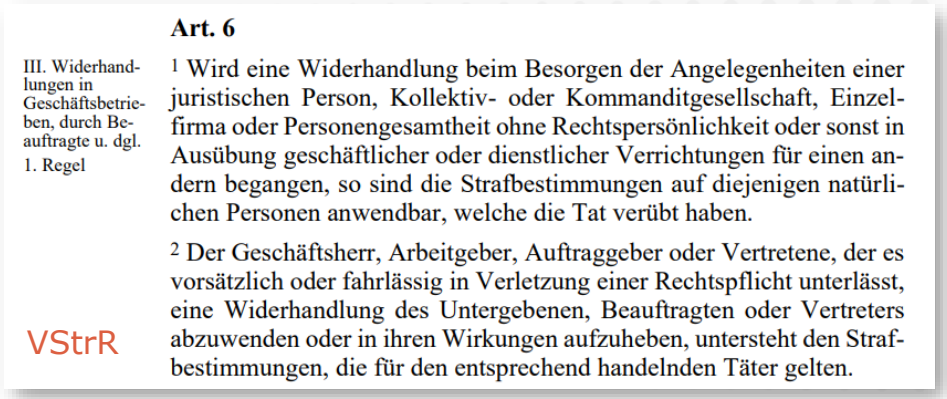
Wer eine Garantenstellung hat

- Wer als GL-Mitglied nicht dafür sorgt, dass Auskunftsersuchen richtig behandelt werden
- Wer als leitender Inhaber einer Bearbeitung keine korrekte DSE in Auftrag gibt
- Der untätige VR, weil er keinen Bericht will

1. Person muss Pflicht haben, Rechtsverletzungen zu verhindern und die dafür nötigen Befugnisse
2. Sie kommt ihrer Pflicht zur sorgfältigen Auswahl, Instruktion und Überwachung nicht nach

Datenschutzstelle: Weisungs-/Interventionsrecht?

- Ermöglicht **Durchsetzung** der Datenschutz-Compliance
- Aber:
  - Führt zu unnötigen internen **Konflikten**
  - Führt zu strafrechtlicher **Verantwortlichkeit**



Art. 6

III. Widerhandlungen in Geschäftsbetrieben, durch Beauftragte u. dgl.

1. Regel

[1] Wird eine Widerhandlung beim Besorgen der Angelegenheiten einer juristischen Person, Kollektiv- oder Kommanditgesellschaft, Einzelfirma oder Personengesamtheit ohne Rechtspersönlichkeit oder sonst in Ausübung geschäftlicher oder dienstlicher Verrichtungen für einen andern begangen, so sind die Strafbestimmungen auf diejenigen natürlichen Personen anwendbar, welche die Tat verübt haben.

[2] Der Geschäftsherr, Arbeitgeber, Auftraggeber oder Vertretene, der es vorsätzlich oder fahrlässig in Verletzung einer Rechtspflicht unterlässt, eine Widerhandlung des Untergebenen, Beauftragten oder Vertreters abzuwenden oder in ihren Wirkungen aufzuheben, untersteht den Strafbestimmungen, die für den entsprechend handelnden Täter gelten.

VStrR

Pflicht zur Überwachung
+
Entscheidungsgewalt
=
Garantenstellung

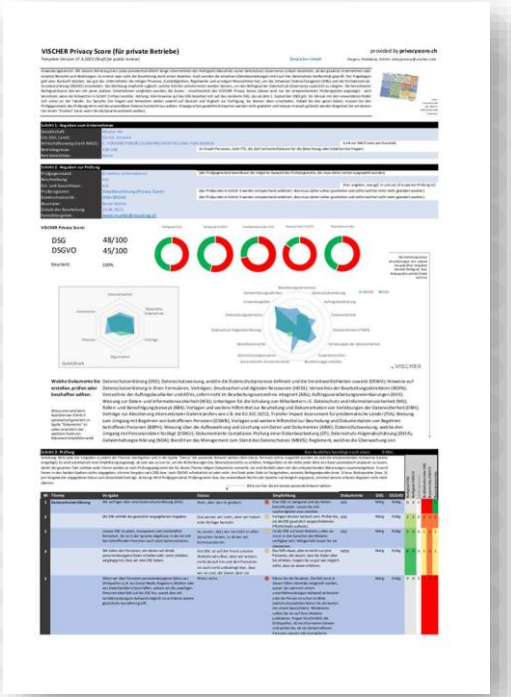
Sicherer: Reines Berichtsrecht an GL/VR

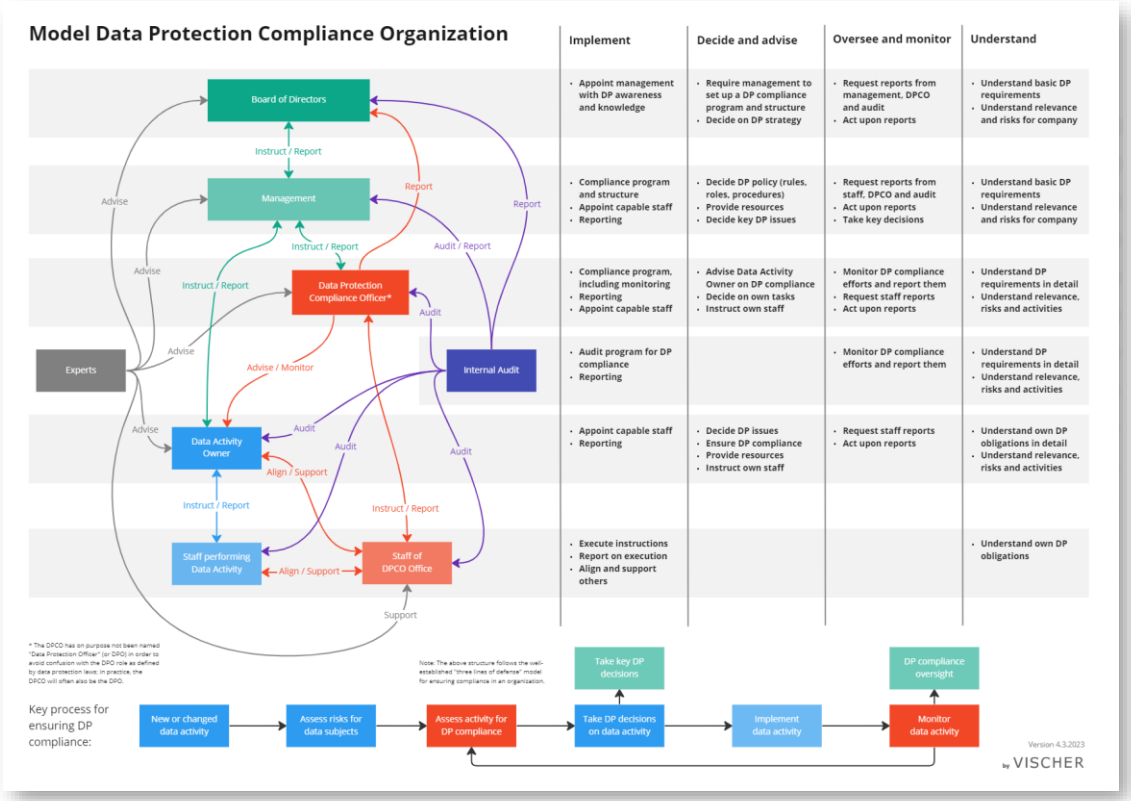
Pflichten der GL bzw. des VR

- Angemessene …
  - **Auswahl**
  - **Instruktion** (inkl. Bereitstellung von Ressourcen)
  - **Überwachung**

- Es genügt nicht, die GL mit der Umsetzung des Datenschutzgesetzes zu beauftragen
  - VR muss sich **berichten lassen** (GL auch)
  - **Durch DPCO**, direkt oder indirekt via Compliance

Beispiel:
https://privacyscore.ch (oder Excel)





Optimalerweise sind (mittlere und grössere) Unternehmen so aufgestellt.

https://www.rosenthal.ch/downloads/VISCHER-data-protection-compliance-organization.pdf

VISCHER

Danke für Ihre Aufmerksamkeit!

Fragen: drosenthal@vischer.com

Weiteres Material:
www.rosenthal.ch

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