scope & focus
Service-Gesellschaft mbH

# Umsetzung der DSGVO in einem „lockeren“ Konzernverbund mit Hilfe der Software verinice

veriniceXP

28.2.2019

1

scope & focus
Service-Gesellschaft mbH

## scope & focus

- Gegründet 2000
- Sitz in Hannover und Bremen
- Schwerpunkt: Datenschutzdienstleistungen

- Mitglied im BvD und GDD
- Aktiv in der BITKOM und im DIN

2

scope & focus Service-Gesellschaft mbH

## Referent

**Dipl. Ök. Stephan Rehfeld**

- externer Datenschutzbeauftragter, Auditor der DQS GmbH
- Stellvertretender Leiter des AK Datenschutz und Identitätsmanagement des DIN
- Stellvertretender Leiter des GDD-Erfa-Kreises Hannover

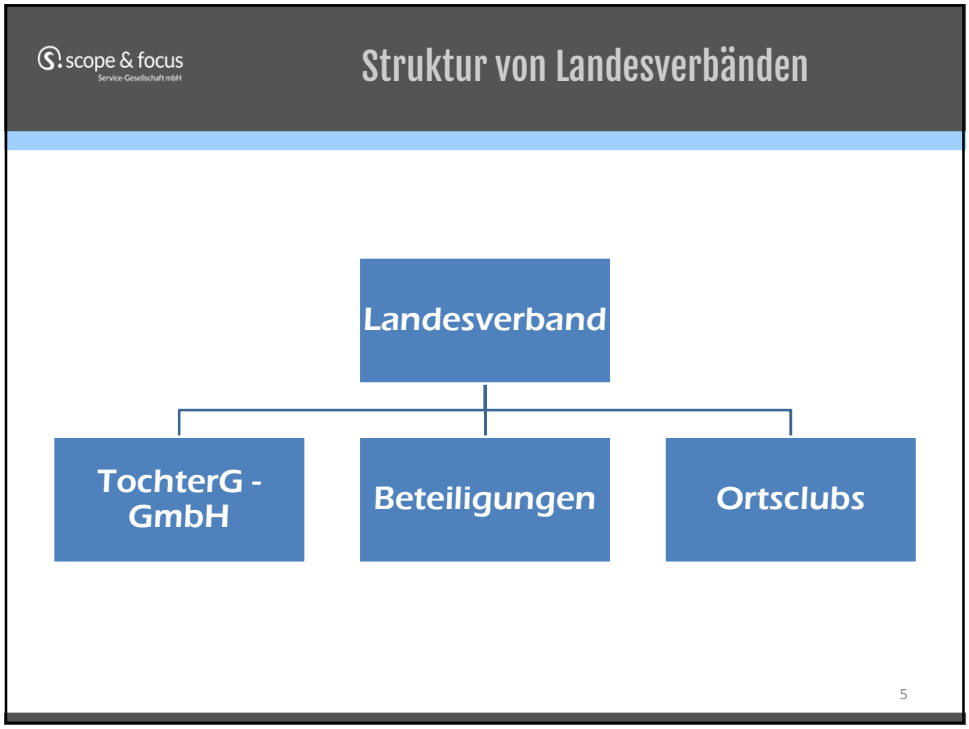
3

scope & focus Service-Gesellschaft mbH

Struktur von Verbänden

## PROBLEMSTELLUNG

4


scope & focus
Service-Gesellschaft mbH
Struktur von Landesverbänden
Landesverband
TochterG - GmbH
Beteiligungen
Ortsclubs
5


scope & focus
Service-Gesellschaft mbH
Stellung von Landes- und Regionalverbänden
Landesverband Niedersachsen Sachsen-Anhalt
Landesverband OWL
Landesverband Südbayern
Dachverband
6

scope & focus
Service-Gesellschaft mbH

## BASIS DES DSMS (PMS)

7

scope & focus
Service-Gesellschaft mbH

## Umsetzung der DSGVO

**ISO-Welt**

- VdA 10010 – kleiner Einstieg
- ISO - High Level Structure
- ISO 9001
- ISO 27001

**Welt des modernen Grundschutzes**

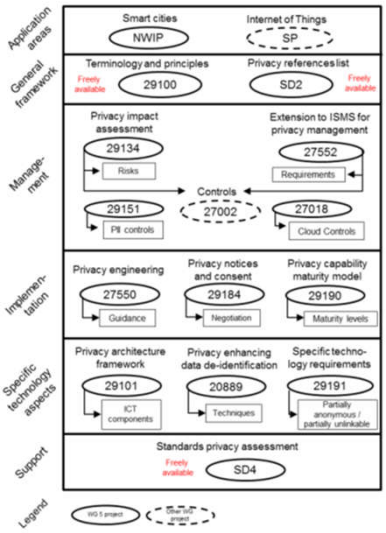
- iDSM 7
- IT-Grundschutz
- Modernisierter Grundschutz

*... oder irgendwas anderes*

8

scope & focus Service-Gesellschaft mbH

## Entscheidung: ISO-Welt



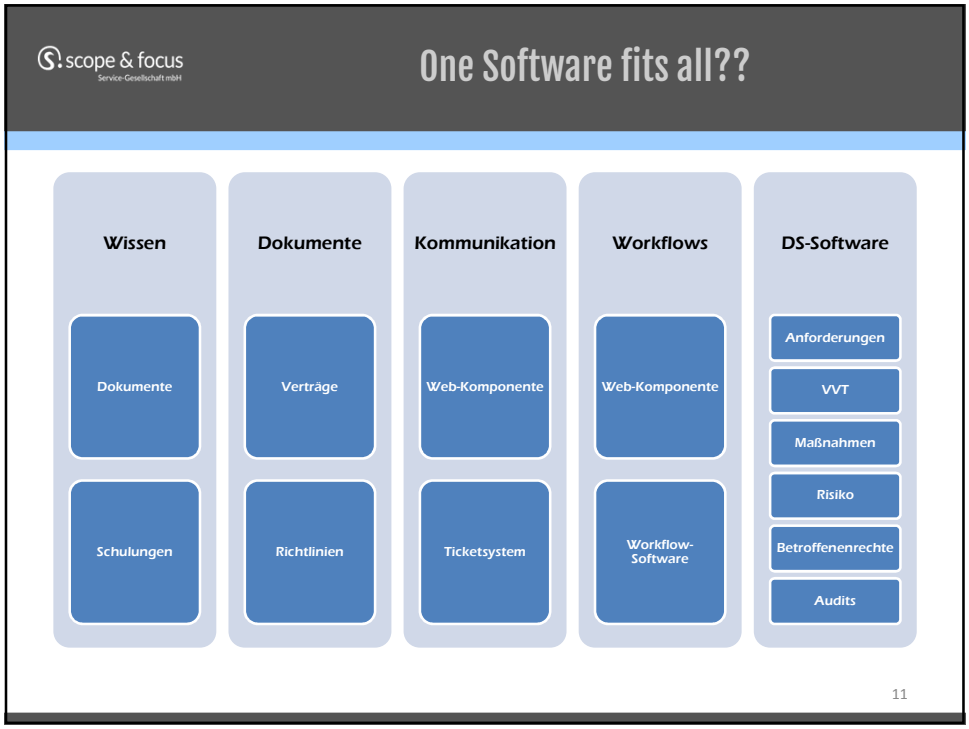

**Quelle: WG 5 SD1 – Overview of Privacy/PII Standards and Projects in SC 27, mainly WG 5**

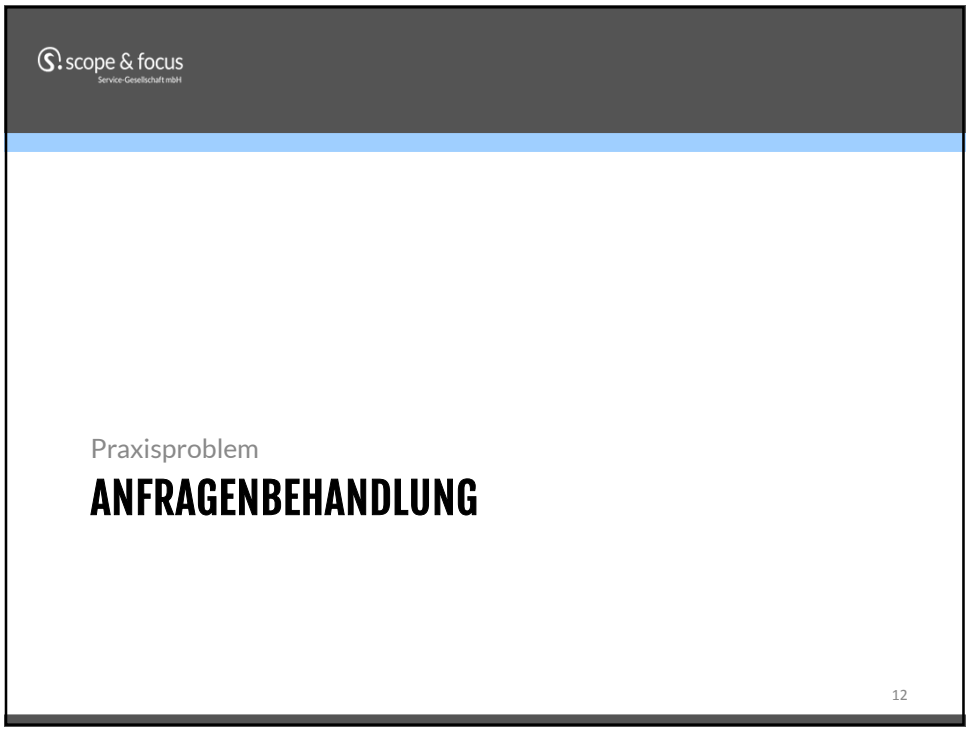
9

scope & focus Service-Gesellschaft mbH

## AUSWAHL DER WERKZEUGE

10


scope & focus
Service-Gesellschaft mbH
One Software fits all??
Wissen
Dokumente
Schulungen
Dokumente
Verträge
Richtlinien
Kommunikation
Web-Komponente
Ticketsystem
Workflows
Web-Komponente
Workflow-Software
DS-Software
Anforderungen
VVT
Maßnahmen
Risiko
Betroffenenrechte
Audits
11

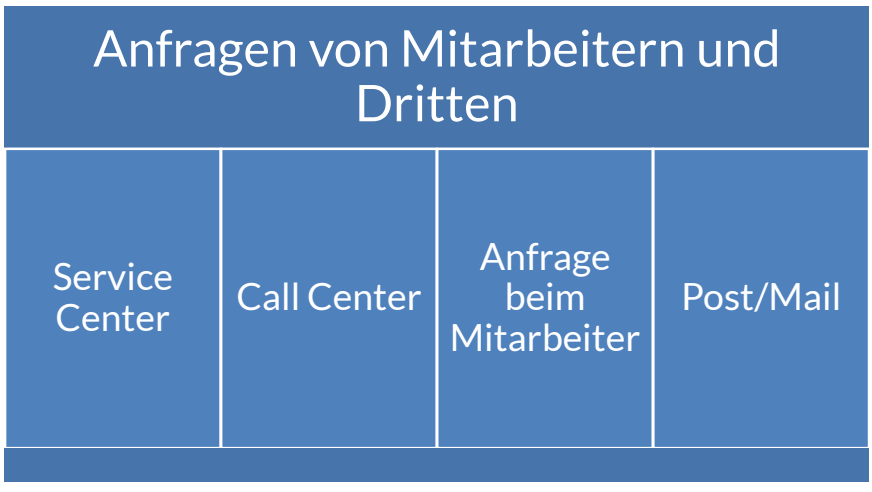

scope & focus
Service-Gesellschaft mbH
Praxisproblem
ANFRAGENBEHANDLUNG
12

## Aufgabenstellung

- Erkennen einer Anfrage durch den Mitarbeiter
- Verteilung einer Anfrage an die richtige Stelle (Beispiel Call Center-Anfrage).
- Beachtung zeitlicher Restriktionen (72 Stunden/1 Monat und SLAs)

13

## Anfragenbehandlung




14

scope & focus Service-Gesellschaft mbH

## Zusammenspiel der eingesetzten Softwares

SerNet verinice.

ep e@sy process

15

scope & focus Service-Gesellschaft mbH

Erfahrungen mit dem

## EINSATZ VON VERINICE

16

scope & focus Service-Gesellschaft mbH

# VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN (VVT)

17

scope & focus Service-Gesellschaft mbH

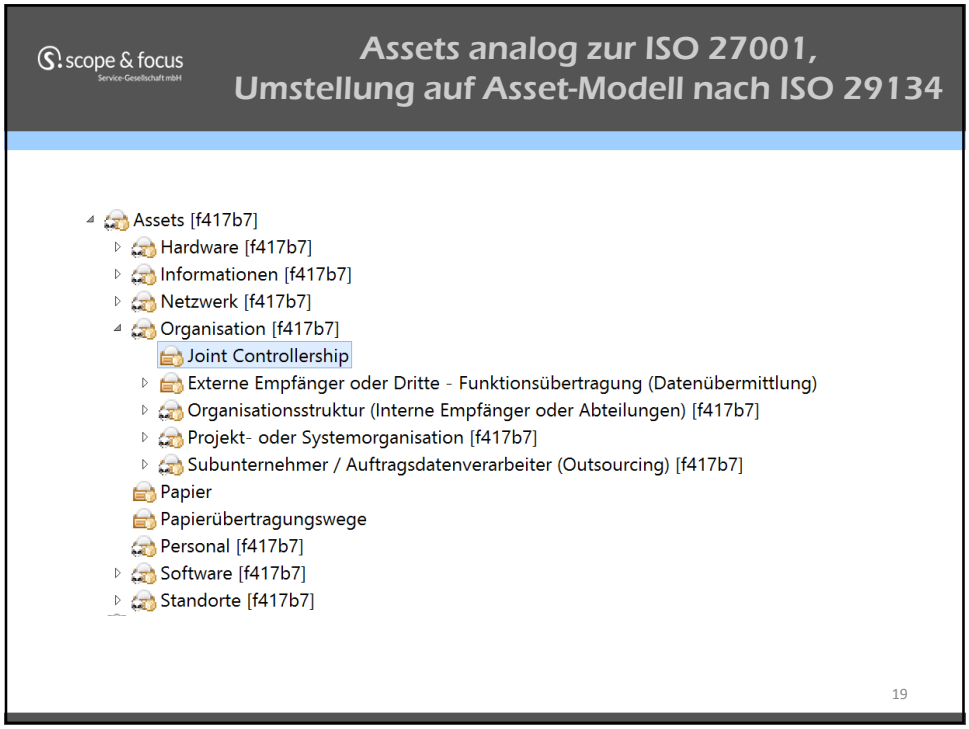
## VVT

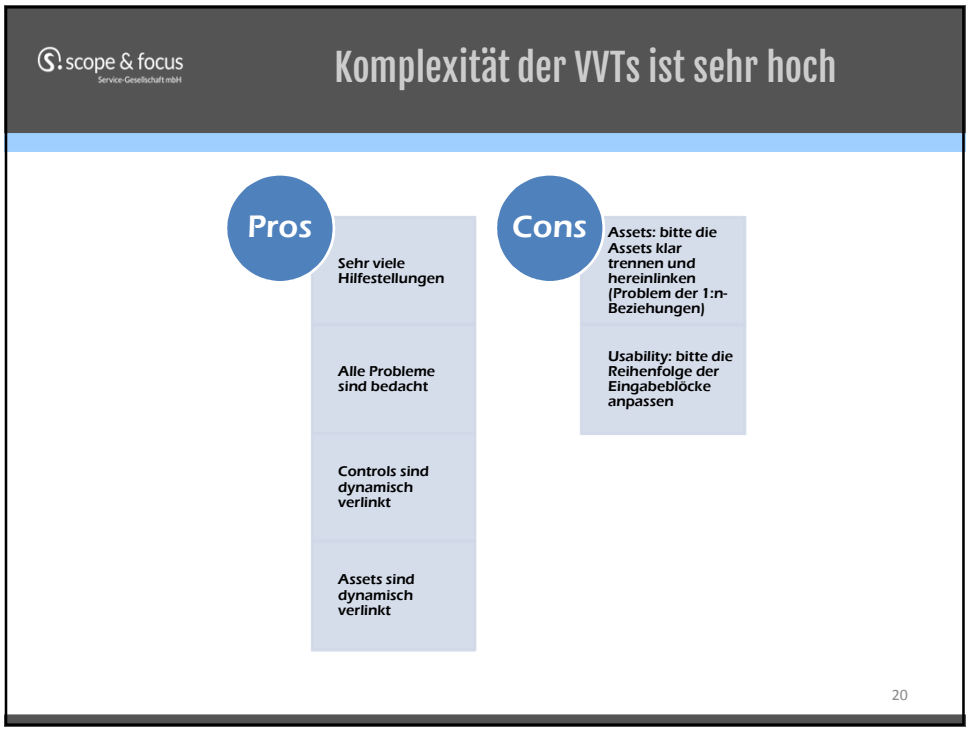
- Prozesse - Verfahrensübersicht [f417b7]
  - 100 Vorstand [f417b7]
  - 200 Geschäftsführung [f417b7]
  - 300 Sekretariat / Assistenz [f417b7]
    - 300-1 Reiseplanung und Veranstaltungen
    - 300-2 interne Versicherungen
    - 300-3 Korrespondenz / Terminvereinbarung
    - 300-4 Vertragsverwaltung
    - 300-5 Reisekostenabrechnung
  - 400 Öffentlichkeitsarbeit [f417b7]
  - 500 Clubdienste [f417b7]
  - 600 Vertrieb/Marketing [f417b7]
  - 700 Verwaltung [f417b7]

**... aber: *Assets werden anders genutzt***

| | | | |
|---|---|---|---|
| benötigt | Beiratsmitglieder | Allgemeiner De... |
| benötigt | Beschäftigte | Allgemeiner De... |
| benötigt | Druckerei | Allgemeiner De... |
| benötigt | Geschäftspartner | Allgemeiner De... |
| benötigt | keine externen Empfänger | Allgemeiner De... |
| benötigt | keine internen Empfänger | Allgemeiner De... |
| benötigt | MS Office Paket | Allgemeiner De... |
| benötigt | Ortsclub-Vorsitzende | Allgemeiner De... |
| benötigt | Reisswolf - Datenträgerv... | Allgemeiner De... |
| benötigt | Vorstand | Allgemeiner De... |

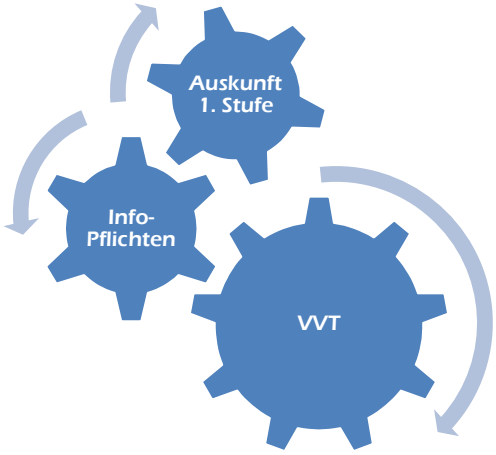
18


scope & focus
Service-Gesellschaft mbH
Assets analog zur ISO 27001,
Umstellung auf Asset-Modell nach ISO 29134
Assets [f417b7]
Hardware [f417b7]
Informationen [f417b7]
Netzwerk [f417b7]
Organisation [f417b7]
Joint Controllership
Externe Empfänger oder Dritte - Funktionsübertragung (Datenübermittlung)
Organisationsstruktur (Interne Empfänger oder Abteilungen) [f417b7]
Projekt- oder Systemorganisation [f417b7]
Subunternehmer / Auftragsdatenverarbeiter (Outsourcing) [f417b7]
Papier
Papierübertragungswege
Personal [f417b7]
Software [f417b7]
Standorte [f417b7]
19


scope & focus
Service-Gesellschaft mbH
Komplexität der VVTs ist sehr hoch
Pros
Sehr viele Hilfestellungen
Alle Probleme sind bedacht
Controls sind dynamisch verlinkt
Assets sind dynamisch verlinkt
Cons
Assets: bitte die Assets klar trennen und hereinlinken (Problem der 1:n-Beziehungen)
Usability: bitte die Reihenfolge der Eingabeblöcke anpassen
20

scope & focus Service-Gesellschaft mbH

## Automatisierte und teilautomatisierte Generierung von Reports aus dem VVT




21

scope & focus Service-Gesellschaft mbH

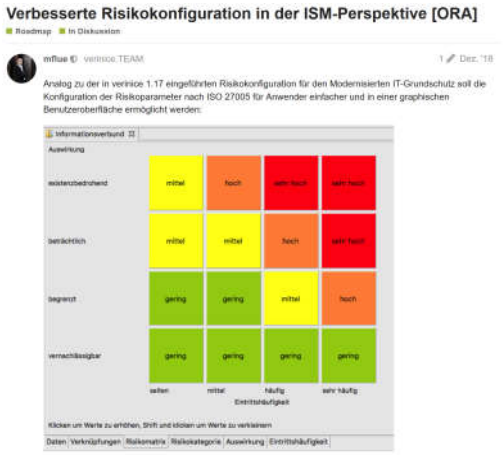
## RISIKO

22

scope & focus Service-Gesellschaft mbH

## Risikoanalyse nach ISO 31000/31010

- Eine Risikoanalyse nach Art. 32 DSGVO ist umsetzbar
- Bitte an sernet:




23

scope & focus Service-Gesellschaft mbH

## Aber Achtung bei DSFAs

### Risikobeispiel: Integrität und Vertraulichkeit

Risiko ID 16

| Risikobeurteilung (gemäß ISO 31000) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| I. Risikoidentifikation | | | | II. Risikoanalyse | | | | III. Risikobewertung |
| Risiko ID | Verarbeitungsgrundsatz (nach Art. 5 DS-GVO) | Risikoquelle | Risikobeschreibung | Möglicher Schaden | Schadenskategorie (nach Erwäg. 75) | Eintrittswahrscheinlichkeit | Schwere des Schadens | Ergebnis |
| 16 | Integrität und Vertraulichkeit | Cyberkrimineller (Hacker/Schadsoftware) | Unbefugte Entwendung der Rohdaten vom Fahrzeug/Versicherten werden aus der Datenbank in Bangladesch entwendet. | Rufschädigung, Diskriminierung, andere wirtschaftliche Schäden | Rufschädigung | Wesentlich (3) | Maximal (4) | sehr hoch (12) |

### Risikobeispiel: Transparenz

Risiko ID 62

| Risikobeurteilung (gemäß ISO 31000) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| I. Risikoidentifikation | | | | II. Risikoanalyse | | | | III. Risikobewertung |
| Risiko ID | Verarbeitungsgrundsatz (nach Art. 5 DS-GVO) | Risikoquelle | Risikobeschreibung | Möglicher Schaden | Schadenskategorie (nach Erwäg. 75) | Eintrittswahrscheinlichkeit | Schwere des Schadens | Ergebnis |
| 62 | Transparenz | Geschäftsführung | Fahrer (ungleich Halter) weiß nichts von der Verarbeitung | Profilbildung durch Bewertung persönlicher Aspekte | Profilbildung durch Bewertung persönlicher Aspekte (Vorlieben, Interessen, Aufenthaltsort, Ortswechsel, etc.) | Maximal (4) | Wesentlich (3) | sehr hoch (12) |

24

scope & focus
Service-Gesellschaft mbH

# CUSTOMIZING

25

scope & focus
Service-Gesellschaft mbH

## Beispiel für Nutzung von Report-Daten

- Prozesse - Verfahrensübersicht [f417b7]
  - 100 Vorstand [f417b7]
  - 200 Geschäftsführung [f417b7]
  - 300 Sekretariat / Assistenz [f417b7]
    - 300-1 Reiseplanung und Veranstaltungen
    - 300-2 Interne Versicherungen
    - 300-3 Korrespondenz / Terminvereinbarung
    - 300-4 Vertragsverwaltung
    - 300-5 Reisekostenabrechnung
  - 400 Öffentlichkeitsarbeit [f417b7]
  - 500 Clubdienste [f417b7]
  - 600 Vertrieb/Marketing [f417b7]
  - 700 Verwaltung [f417b7]

### Transparenz

Nachfolgend finden Sie unsere Transparenzerklärungen:

- Transparenzerklärung Mitgliedschaft
- Transparenzerklärung Mitglieder Service und Beratung
- Transparenzerklärung Mitglieder Service Versicherung
- Transparenzerklärung Mitglieder Service Finanzen
- Transparenzerklärung Buchungen von Reisen
- Transparenzerklärung Warenvertrieb
- Transparenzerklärung ADD Prüfdienst
- Transparenzerklärung Gewinnspiele
- Transparenzhinweis Oldtimer-Veranstaltungen
- Transparenzhinweis Fotos auf Veranstaltungen
- Transparenzhinweis Bewerberverfahren

Antwort auf Auskunftsverlangen mit Recht auf Kopie (Art. 15 DS-GVO)¶

¶

Sehr geehrter [NAME],¶

vielen Dank für Ihre Anfrage vom [DATUM].¶

Wir erheben personenbezogene Daten für die Durchführung einer Mitgliedschaft im ADAC Niedersachsen/Sachsen-Anhalt e.V. (im Weiteren ADAC).¶

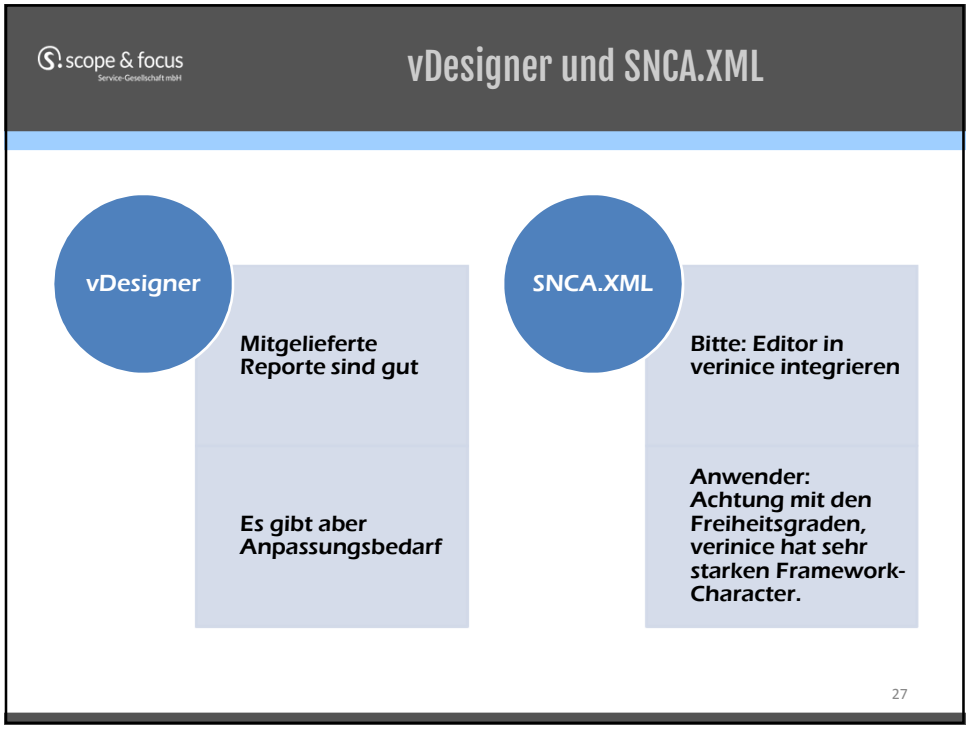
1. Im Rahmen einer ADAC-Mitgliedschaft werden die folgenden personenbezogenen Daten von Mitgliedern und Dritten verarbeitet (sogenannte Auskunft erster Stufe):¶

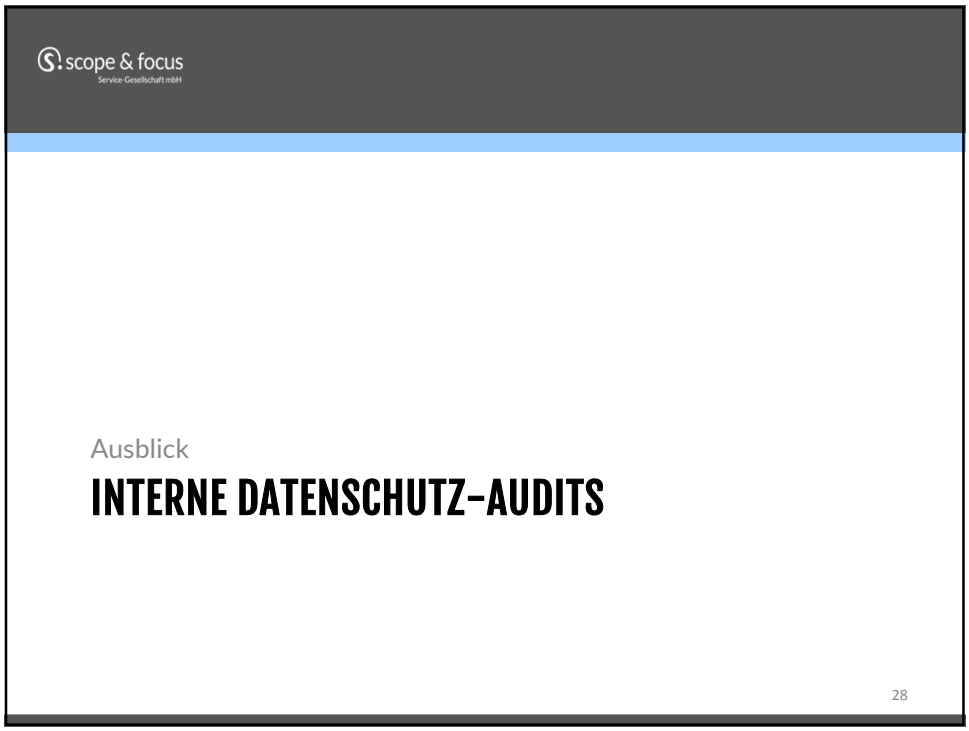
Für die Mitgliedschaft erheben wir unmittelbar von unseren Mitgliedern:¶

- Anrede, Vorname, Name, Geburtsdatum, E-Mail-Adresse, Anschrift und Geschlecht (gemeinsam „Stammdaten“)¶
- Abrechnungs- und Bezahldaten (gemeinsam „Zahlungsdaten“)¶

Die Stammdaten sowie die Zahlungsdaten sind für den Vertragsschluss erforderlich. Wir ordnen unseren Mitgliedern eine Mitgliedsnummer zu, wenn Sie bei uns Mitglied sind.¶

26


scope & focus
Service-Gesellschaft mbH
vDesigner und SNCA.XML
vDesigner
Mitgelieferte Reporte sind gut
Es gibt aber Anpassungsbedarf
SNCA.XML
Bitte: Editor in verinice integrieren
Anwender: Achtung mit den Freiheitsgraden, verinice hat sehr starken Framework-Character.
27


scope & focus
Service-Gesellschaft mbH
Ausblick
INTERNE DATENSCHUTZ-AUDITS
28

scope & focus Service-Gesellschaft mbH

## Reifegradmodell zum Audit der toMs

Datenschutz Reifegradmodell TOMs (Arbeitsgruppe)

Beiträge Mitglieder Kalender Dateien Webdokumente Profil

A Text Bild ? Frage Termin
Beitrag verfassen

Alle Ungelesen Erwähnt Entdecken Filter

Rebekka Weiß
Nächste TK zum Reifegradmodell TOMs
Freitag, 15. März 2019 - 15:30 bis 18:00 Uhr

Liebe Mitglieder,

gern lade ich Sie hier zur nächsten TK zur Weiterarbeit am Reifegradmodell TOMs ein. Wie heute im Call besprochen findet der nächste Call am 15. März von 15:30 bis 18:00 Uhr statt (wir nehmen uns etwas mehr Zeit, da viele offene Kapitel auf

Sehr geehrter Herr Rehfeld,

ich möchte Sie herzlich auf die nächste Sitzung des AK Datenschutz aufmerksam machen. Wir treffen uns am

**Donnerstag, 28. März 2019, 09:30 – 16:30 Uhr**
**Haus der Wirtschaft – Wiesenstraße 35 – 45473 Mühlheim an der Ruhr**
Nähere Anreiseinformationen finden Sie unter hier, die Anreise von Düsseldorf dauert mit ÖPNV bzw. PKW circa 35 Minuten. Eine Liste mit Hotelempfehlungen für Mühlheim finden Sie anbei.

Wir danken Heiko Gossen und der migosens GmbH für die Gastfreundschaft.

**Im Mittelpunkt der Sitzung werden aktuelle Umsetzungsthemen der Datenschutzgrundverordnung (insbesondere TOMs, Beschäftigtendatenschutz, Informationspflichten & Icons, Zertifizierung und Auftragsverarbeitung) sowie die in Arbeit befindlichen regulatorischen Vorschläge (E-Evidence Vorschlag, ePrivacy Verordnung, Datenschutzomnibus) stehen.** Die komplette Agenda versenden wir zeitnah mit der Einladung.

29

scope & focus Service-Gesellschaft mbH

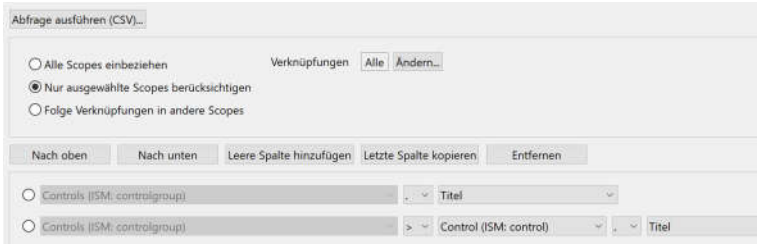
(nicht verwechseln mit Datenportabilität)

## DATENAUSTAUSCH IN EINER HETEROGENEN UMGEBUNG

30

scope & focus Service-Gesellschaft mbH

## Report-Abfrage




31

scope & focus Service-Gesellschaft mbH

scope & focus

Ihre Daten - mit Sicherheit!

Leonhardtstr. 2
30175 Hannover
T: 0511 | 364 221-0
F: 0511 | 364 221-99

Hoerneckestr. 19-21
28217 Bremen
T: 0421 | 369 3530-0
F: 0421 | 369 3530-99

www.scope-and-focus.com
information@scope-and-focus.com

Dipl.-Ök. Stephan Rehfeld

32