activeMind.AG

Informationssicherheit nach DS-GVO

Klaus Foitzick
Vorstand activeMind AG
München, 12. und 19. März 2018

IHK München und Oberbayern

Wann gilt die DS-GVO?

Sachlich

Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten …

örtlich

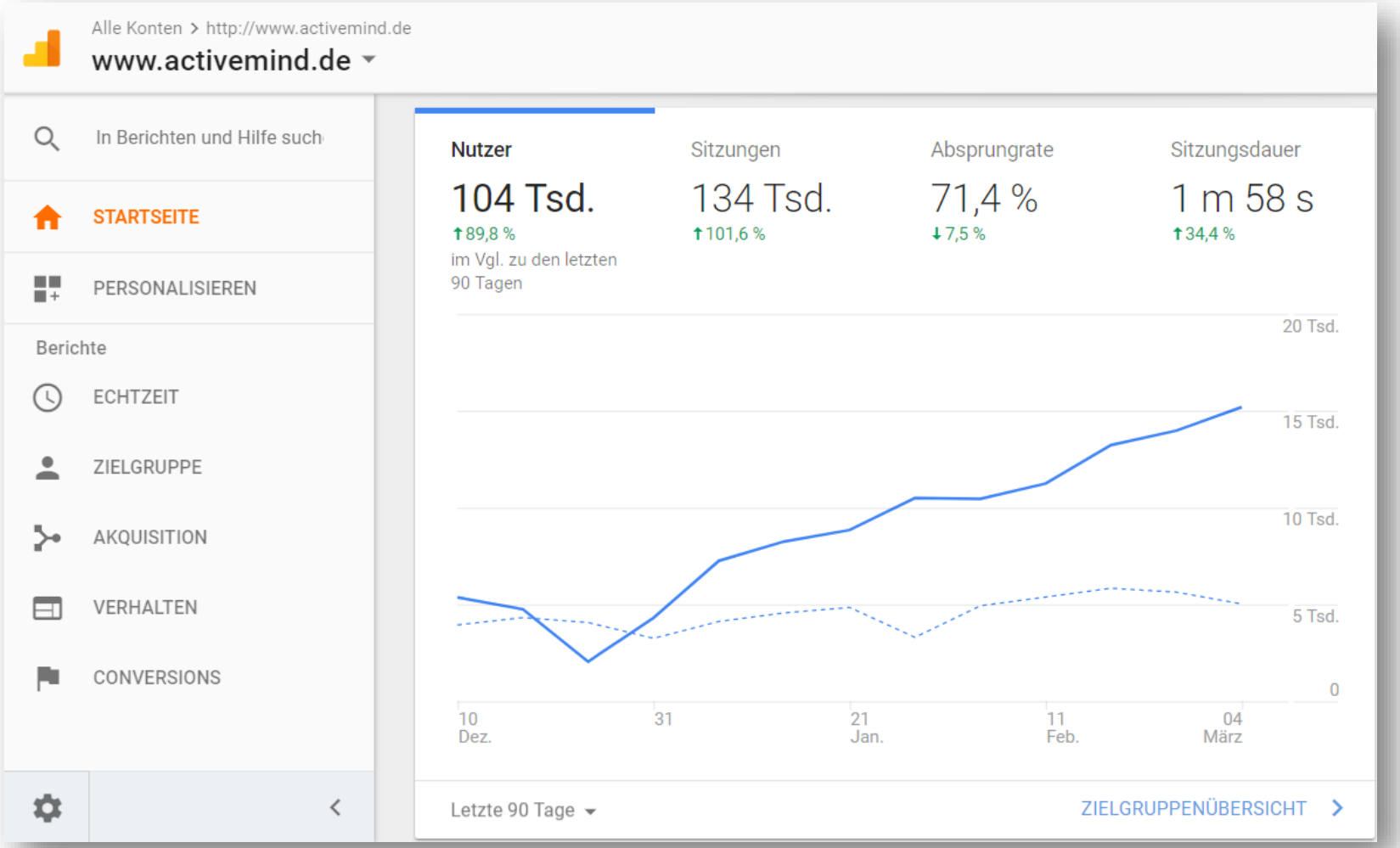
…soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet … oder die Datenverarbeitung erstreckt sich auf Betroffene in der Union die Waren oder Dienstleistung von außerhalb der Union beziehen.

Zentraler Begriff „personenbezogene Daten“

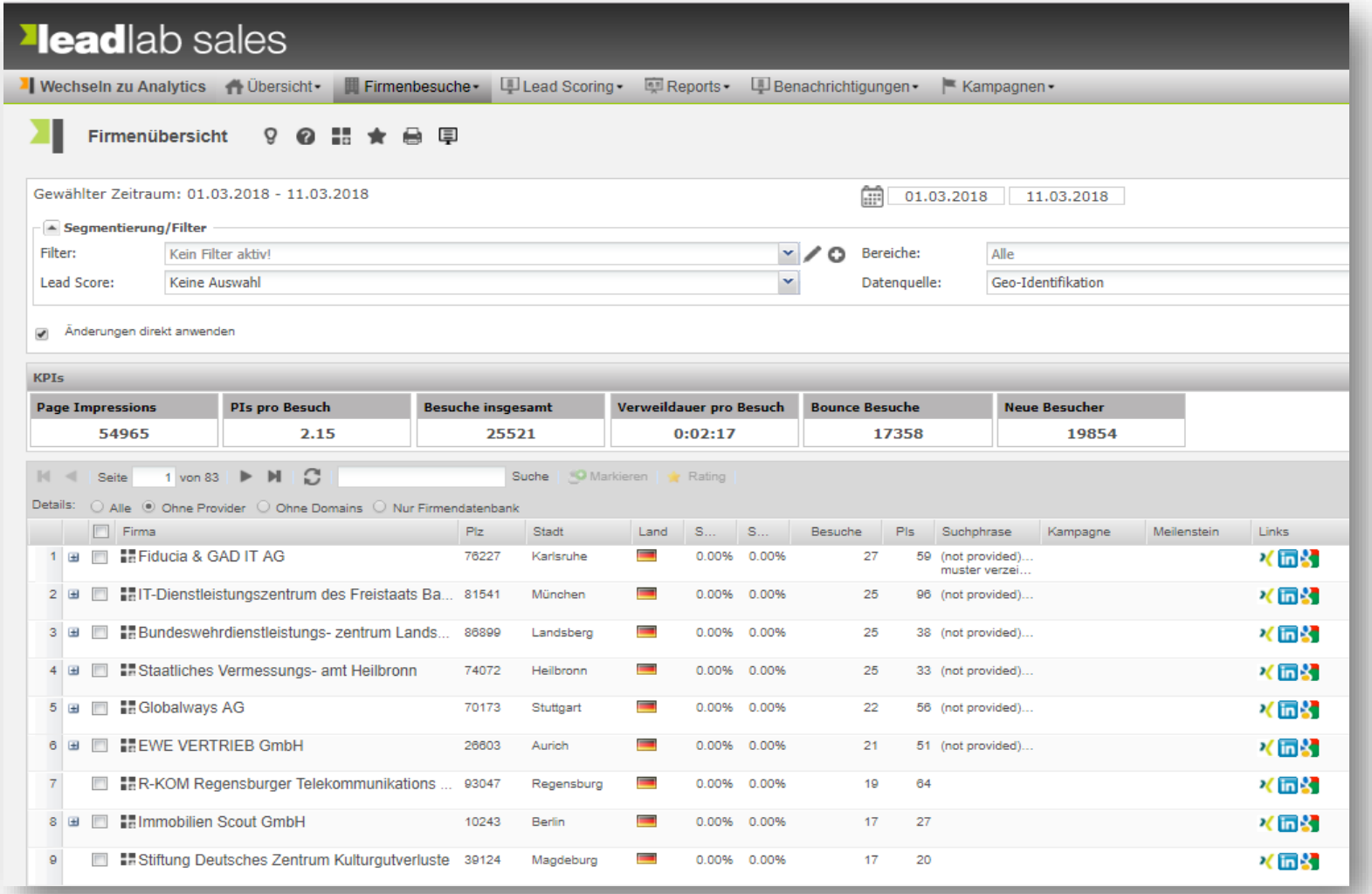
„personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen…

einfach, oder?

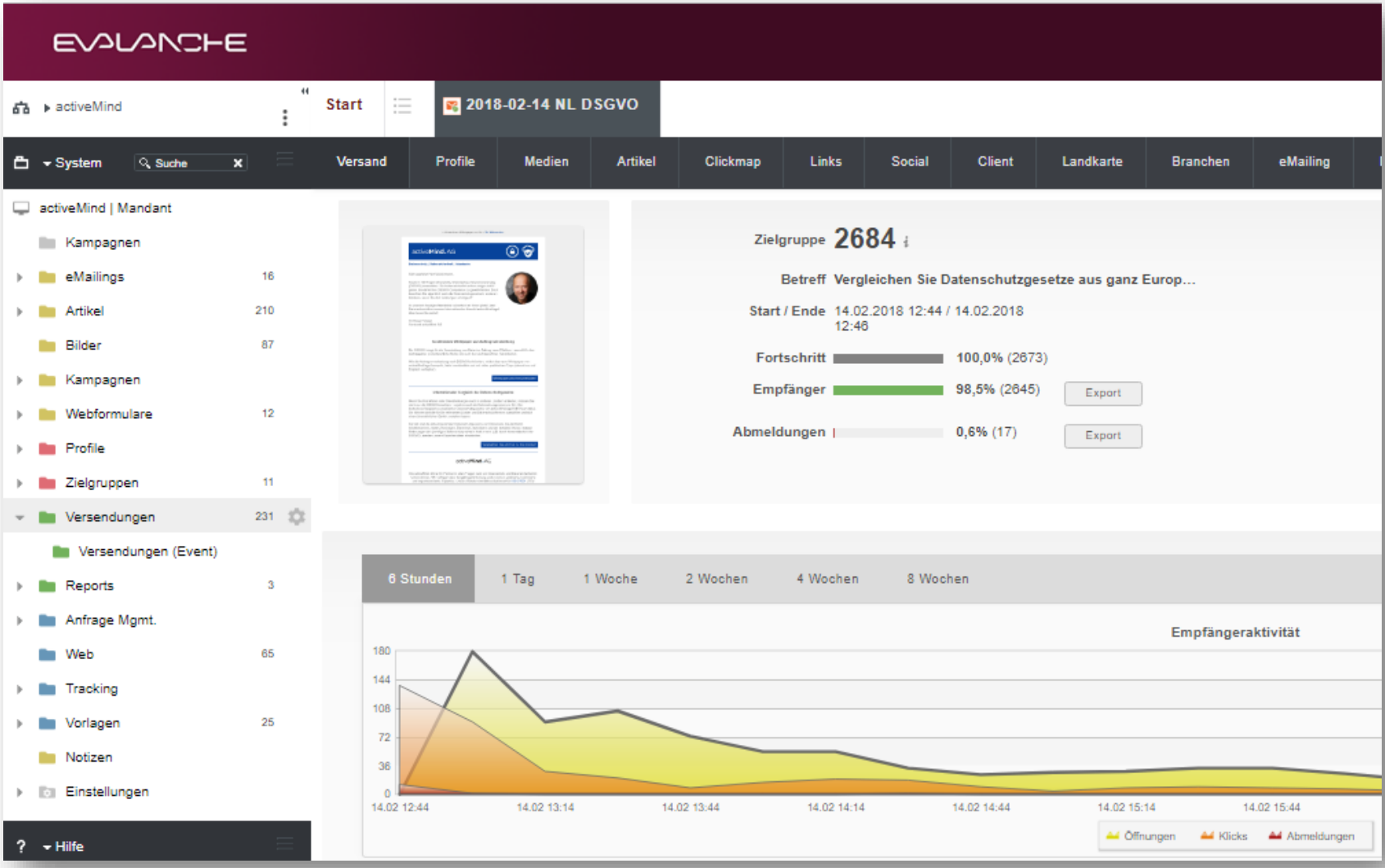
Anwendbarkeit bei Google Analytics? (Webanalyse)



Anwendbarkeit bei Wiredminds.de? (Webanalyse)



Anwendbarkeit bei Evalanche? (Newslettersystem)



Ergebnis

- Sachliche Anwendbarkeit
  - Bestimmbarkeit einer Person (auch wenn nur durch andere) ausreichend
- Örtliche Anwendbarkeit
  - Es gilt der **Marktort** und damit an dem Ort an dem der Verantwortliche oder der Dienstleister seine Tätigkeit ausführt

→ DS-GVO bei diesen Tools anwendbar

Sobald DS-GVO anwendbar

→ sind Grundprinzipien für die Verarbeitungen einzuhalten

Grundprinzipien für Verarbeitungen (Art. 5 DS-GVO)

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
  …Verbot mit Erlaubnisvorbehalt, Verhältnismäßigkeit, Information
- **Zweckbindung**
  …für festgelegte, eindeutige und rechtmäßige Zwecke.
- **Datensparsamkeit**
  …auf das notwendige Maß beschränkt.
- **Richtigkeit**
  …sachlich richtig.
- **Speicherbegrenzung**
  …zeitlich erforderlich.
- **Datensicherheit**
  …angemessene Sicherheit („Integrität“ und „Vertraulichkeit“)
- **Rechenschaftspflicht**
  Der Verantwortliche ist für die Einhaltung dieser Regeln verantwortlich und muss diese nachweisen können.

Zu abstrakt?

Grundprinzipien (Bsp. Kameraufzeichung am Firmeneingang)

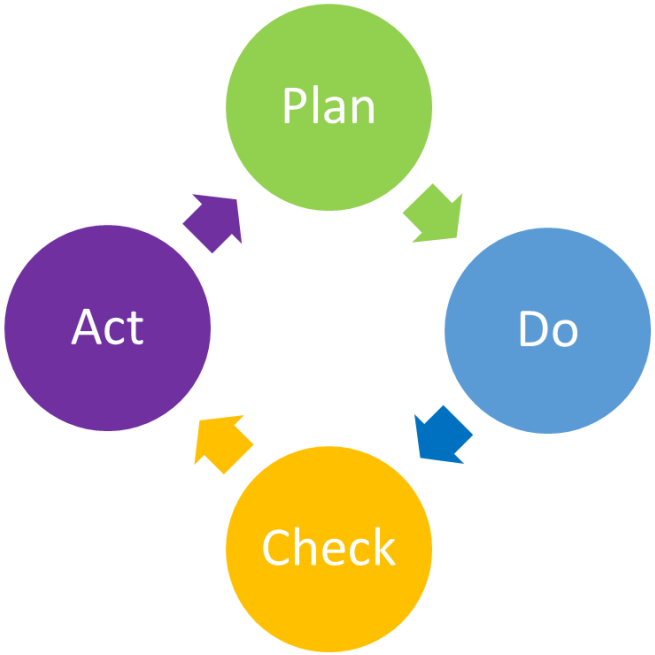
Grundprinzip	Prüfung
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	Wahrung berechtigter Interessen, Erforderlichkeit, Interessenabwägung, Drittinteresse, Geeignetheit, Erwartungshorizont, Piktogramm, Hinweise auf: Identität des Verantwortlichen, DSB, Zweck, Rechtsgrundlage, berechtigtes Interesse, Speicherdauer, Auskunftsrecht, Beschwerderecht, ggf. Empfänger
Zweckbindung	Nur für den im Voraus festgelegten Zweck nutzen
Datensparsamkeit	Bereiche ausblenden, Zeitrahmen festlegen
Richtigkeit	Zuordnung: Kamera, Ort und Zeit sicherstellen
Speicherbegrenzung	48 Stunden (Privacy by design / default)
Datensicherheit	Zugriffssteuerung, Verschlüsselung
Rechenschaftspflicht	Regelung / Umsetzung / Kontrolle / Korrektur

Bay. Landesamt: https://www.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf

Seine Rechenschaftspflicht zwingt den Verantwortlichen zum Aufbau eines

Datenschutz-Managementsystems

Rechenschaftspflicht
=> Managementsystem



- **Alle Prozesse müssen**
  - Nachweislich geregelt und dokumentiert sein:
    → **Planung (plan)**
  - Auf Basis der Regelung gesteuert umgesetzt werden:
    → **Umsetzung (do)**
  - Gemessen werden (Erfolg, Wirksamkeit):
    → **Kontrolle (check)**
  - Bei Abweichungen korrigiert werden:
    → **Verbesserung (act)**

Managementaufgaben

(1) **Identifikation der eingesetzten Verfahren** und gesetzlichen Anforderungen

(2) **Vorgaben** für die Verarbeitung, Festlegen der **Verantwortlichkeiten**

(3) **Planung** der Umsetzung (Tech./ Org.)

(4) Ressourcen, **Kompetenzen, Schulung** und Dokumentation

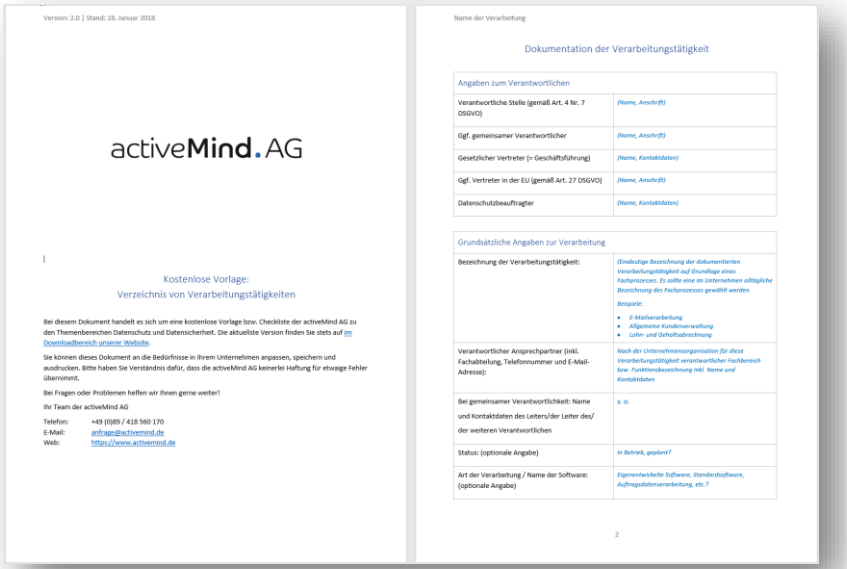
(5) **Betrieb** (Techn./Org. Maßnahmen zur risikoorientierten IT-Nutzung, Pseudonymisierung, Verschlüsselung, Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit, Resilenz

(6) Nachweisbare **Kontrolle, Tätigkeitsbericht**

Entspricht Struktur ISO 9001 / 27001 / 14001 (ggf. nutzen)

(1) Dokumentation der Verfahren (Art. 30 DS-GVO)

- Prüfung der Rechtsgrundlage
- Prüfung der datenschutzrechtlichen Grundsätze
- Risikobewertung, um die Verhältnismäßigkeit der techn. – org Maßnahmen zu bewerten
- Identifikation eingesetzter Dienstleister mit oder ohne entsprechende AV-Verträge
- Identifikation von ggf. bestehenden Drittlandstransfers
- Integration in ein entsprechendes Löschkonzept
- Schwellwertanalyse zur Datenschutzfolgeabschätzung
- Erfüllung der Informationspflichten

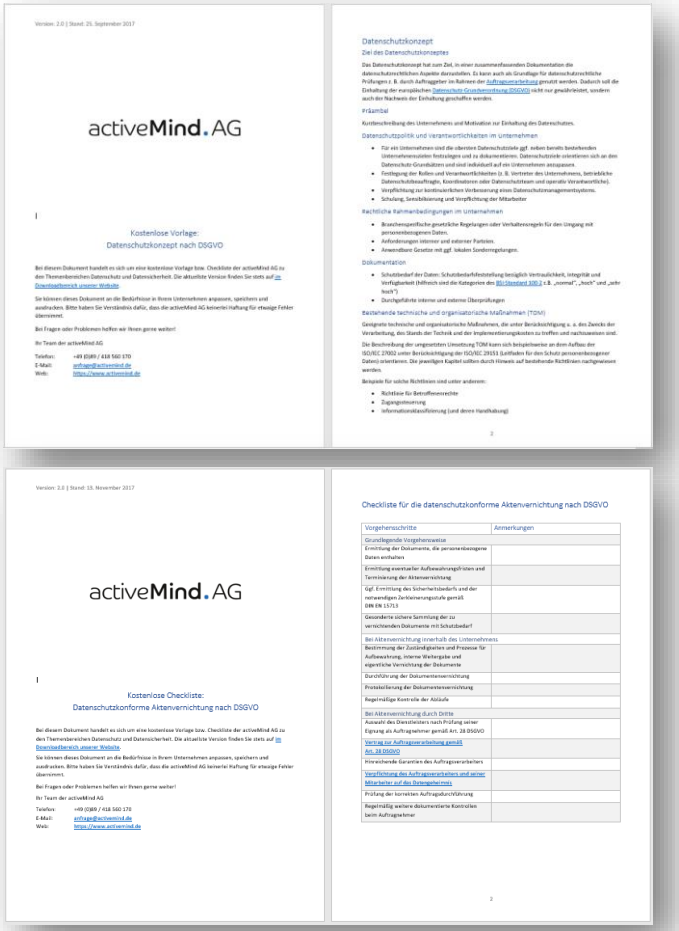


Vorlage: https://www.activemind.de/datenschutz/dokumente/verfahrensverzeichnis/
https://www.activemind.de/datenschutz/datenschutzhinweis-generator/

(2) Vorgaben für die Verarbeitung (Beispielvorlagen)

- Datenschutzkonzept
  mit technischer Umsetzung

- Datenschutzkonforme
  Aktenvernichtung
  mit technischer Umsetzung

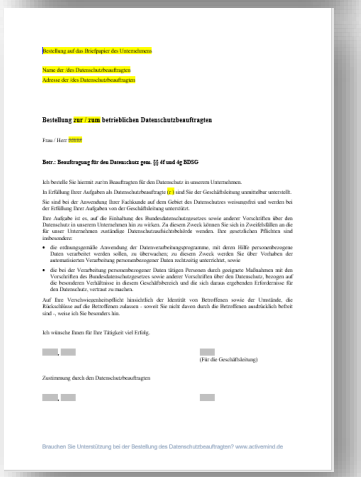


Vorlagen: https://www.activemind.de/datenschutz/dokumente/datenschutzkonzept/
https://www.activemind.de/datenschutz/dokumente/aktenvernichtung/

(2) Verantwortlichkeiten

- Betrieblicher Datenschutzbeauftragter
  - allg. Voraussetzungen
    u.a technische Qualifikation

- Bestellungsdokument Datenschutzbeauftragter
  - Aufgaben

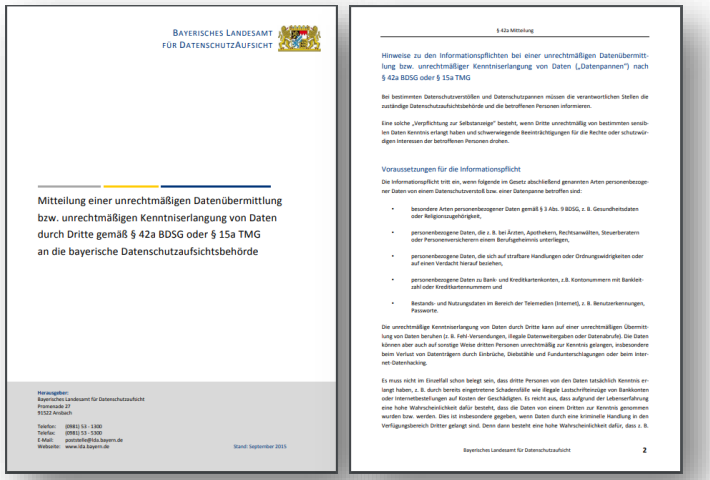


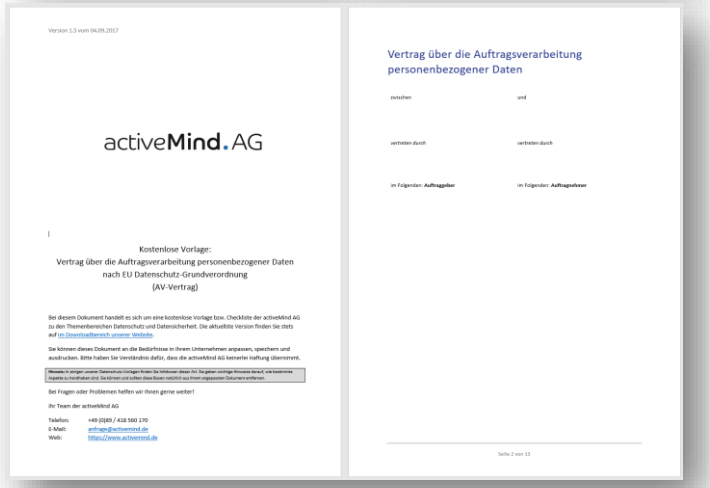
Vorlagen: https://www.activemind.de/datenschutz/dokumente/bestellung-datenschutzbeauftragter/
https://www.activemind.de/datenschutz/dokumente/dsb-dsgvo/

(3) Planung (Beispielvorlagen)

- Notfallplan
  bei Datenschutzvorfall
  - Technische Meldewege / Fristen

- Vertrag
  zur Auftragsverarbeitung
  - Datenschutzgarantien





Links: https://www.lda.bayern.de/media/info_42a_mitteilung.pdf
https://www.activemind.de/datenschutz/dokumente/av-vertrag/

(4) Schulung

- Datenschutzbeauftragter (IHK)
  - Praktische Umsetzung
  - Kundendaten
  - Beschäftigtendaten
  - Informationssicherheit

IHK Akademie
München und Oberbayern

FACHSEMINAR

Datenschutzbeauftragte/-r IHK

Nutzen

Ihre Qualifizierung für die Zukunft - Datenschutzbeauftragte/-r IHK! Die Umsetzung der datenschutzrechtlichen Verpflichtungen ist für viele Unternehmen eine größere Herausforderung. Zeitgleich wächst der Umsetzungsdruck, sei es durch veränderte Märkte oder Aufsichtsbehörden. Deshalb hat der Gesetzgeber zur Unterstützung der Geschäftsführung den betrieblichen Datenschutzbeauftragten vorgesehen oder sogar vorgeschrieben. Sein Profil ist klar definiert: Die Aufgabe darf nur übernehmen, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Erwerben Sie mit dieser Seminarreihe alle erforderliche Fachkenntnisse des Datenschutzbeauftragten. Holen Sie sich praxisnahe Hilfestellung bei der Erfüllung ihrer Aufgaben. Nach dem erfolgreichen, in allen Branchen anerkannten Abschluss sind Sie zertifizierte/-r Datenschutzbeauftragte/-r IHK. Eine Fortbildungsveranstaltung gemäß §4F Abs. 3 BDSG.

Zielgruppe

Geeignet für Unternehmenslenkungen, Datenschutzbeauftragte oder Personen, die sich in das Themengebiet "betriebliche Datenschutzbeauftragte" praktisch einarbeiten wollen.

Veranstaltungsinhalt im Überblick

Die Weiterbildung bietet bestellten oder künftigen Datenschutzbeauftragten die Möglichkeit zum Erwerb der erforderlichen Grundkenntnisse oder deren Vertiefung. Zudem können Teilnehmer ihr Wissen belegen, da sie in allen Veranstaltungen an einem Zertifikatstest teilnehmen können. Nach erfolgreicher Prüfung wird automatisch ein IHK-Zertifikat ausgestellt, das die Ausbildung bestätigt. Themen der 4 Basisveranstaltungen für den Abschluss:

- Seminar 1: Einstieg leicht gemacht: Praktische Umsetzung des Datenschutzes nach BDSG und DSGVO (2 Tage)
- Seminar 2: Kundendaten und Datenschutz (1 Tag)
- Seminar 3: Beschäftigtendaten und Datenschutz (1 Tag)
- Seminar 4: Datensicherheit und Datenschutz (1 Tag)

Veranstalter

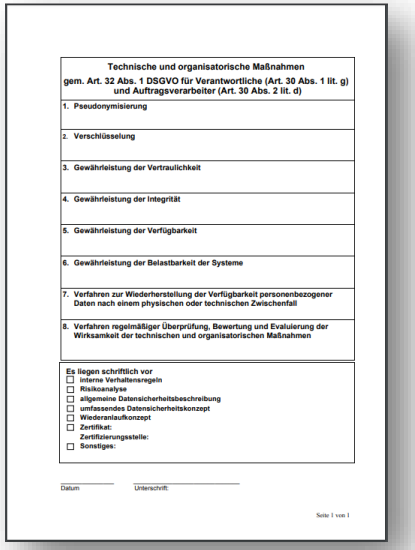
IHK Akademie München und Oberbayern gGmbH

Link: https://akademie.muenchen.ihk.de/datenschutz-sicherheit/datenschutzbeauftragte-r-ihk/

(5) Technische und organisatorische Maßnahmen

Die DSGVO verpflichtet Verarbeiter von personenbezogenen Daten in Art. 32 dazu, „geeignete technische und organisatorische Maßnahmen [zu treffen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“.

8 Gebote des BDSG gibt es nicht mehr, sondern Schutzziele:



Technische und organisatorische Maßnahmen
gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

1. Pseudonymisierung
2. Verschlüsselung
3. Gewährleistung der Vertraulichkeit
4. Gewährleistung der Integrität
5. Gewährleistung der Verfügbarkeit
6. Gewährleistung der Belastbarkeit der Systeme
7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall
8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Es liegen schriftlich vor
- ☐ interne Verhaltensregeln
- ☐ Risikoanalyse
- ☐ allgemeine Datensicherheitsbeschreibung
- ☐ umfassendes Datensicherheitskonzept
- ☐ Wiederanlaufkonzept
- ☐ Zertifikat:
  Zertifizierungsstelle:
- ☐ Sonstiges:

Datum Unterschrift

Seite 1 von 1

- Pseudonymisierung;
- Verschlüsselung;
- Gewährleistung der Vertraulichkeit;
- Gewährleistung der Integrität;
- Gewährleistung der Verfügbarkeit;
- Gewährleistung der Belastbarkeit der Systeme;
- Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall;
- Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Vorlage: https://www.bvdnet.de/wp-content/uploads/2017/06/Muster_Verz_der_Verarbeitungst%C3%A4tigkeiten_TOMs.pdf

(5) Betrieb: Beispielhafte Umsetzung (webshop)

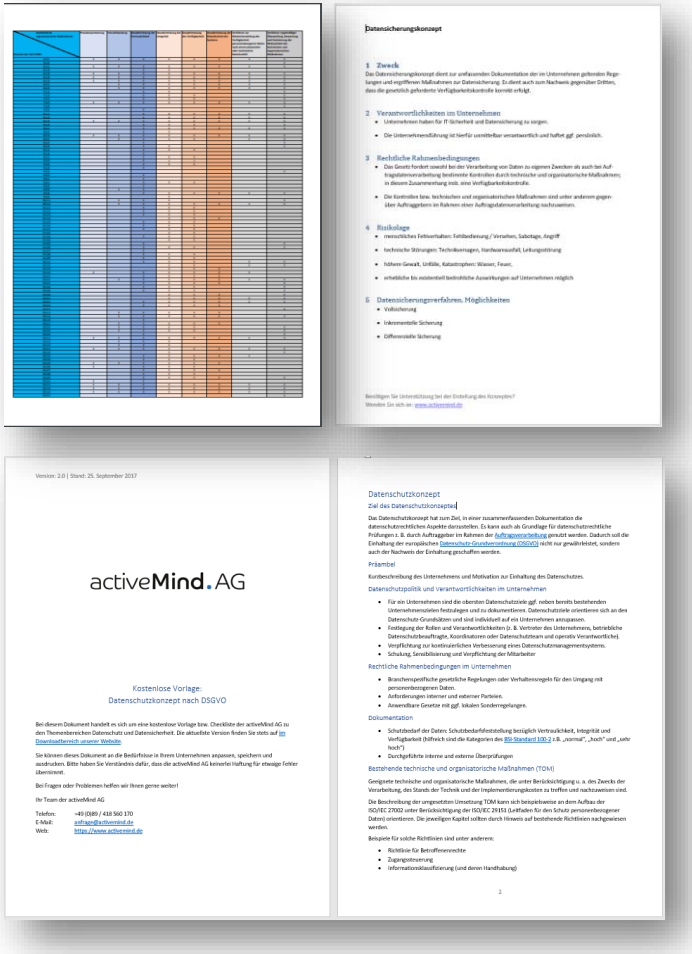
Schutzziel	Beispielhafte Umsetzung
Pseudonymisierung	Kundenverwaltung über BenutzerID
Verschlüsselung	Verschlüsselte Webseite / Backups
Gewährleistung der Vertraulichkeit	Verpflichtung Personal / DL / Zugriffskonzept / Firewall / IPS
Gewährleistung der Integrität	Technischer Integritätsschutz (HASH), Eingabe Prüfung
Gewährleistung der Verfügbarkeit	Backupkonzept / Replikationskonzept
Gewährleistung der Belastbarkeit	Realtime Überwachung / automatisierte Reaktion auf Störung mit Eskalation / § 13 VII TMG
Verfahren zur Wiederherstellung	Notfallplan zur Wiederherstellung / mit Prüfung
Überprüfung der Wirksamkeit	Penetrationstest (White BOX / Black BOX) internes Audit durch unabhängigen qualifizierten Prüfer

Orientierung an technischen Standards empfehlenswert. Beispiel ISO 27002, ISO 29151

(5) Betrieb (Beispielvorlagen)

- Kreuzreferenz
  Schutzziele ⟺ ISO 27002
- Datensicherungskonzept

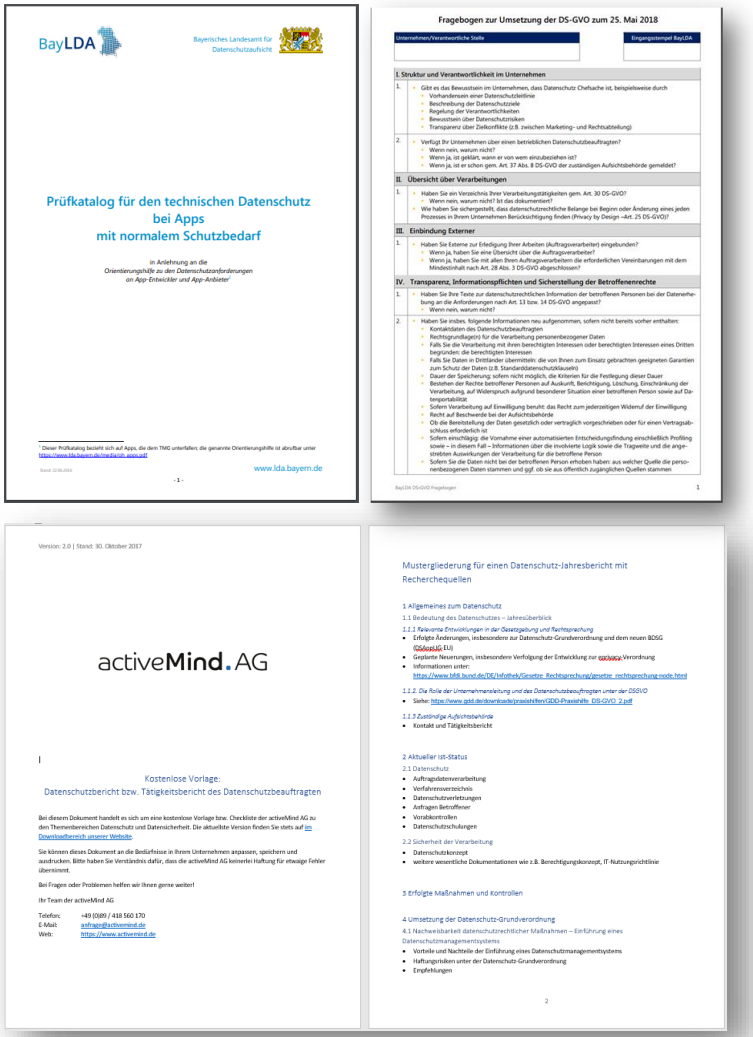
- Datenschutzkonzept
  - Organisatorische Vorlagen
  - Verantwortlichkeiten
  - Technische Maßnahmen



Vorlagen: https://www.activemind.de/datenschutz/dokumente/datenschutzkonzept/
https://www.activemind.de/datenschutz/dokumente/datensicherungskonzept/
https://www.activemind.de/magazin/technische-organisatorische-massnahmen-dsgvo/

(6) Kontrolle und Tätigkeitsbericht (Beispielvorlagen)

- Prüfkatalog DS-GVO
- Prüfkatalog bei Apps
  - Verschlüsselung
  - Zugriffskontrolle
  - Datenübertragung
- Tätigkeitsbericht



Vorlagen: https://www.activemind.de/magazin/baylda-prueft-umsetzung-dsgvo/
https://www.lda.bayern.de/media/baylda_pruefkatalog_apps.pdf
https://www.activemind.de/datenschutz/dokumente/datenschutzbericht/

Fazit zur Informationssicherheit in der DS-GVO

- Die DS-GVO fordert grundsätzlich keine „neuen“ technischen Maßnahmen, sondern deren Einbindung in ein risikoorientiertes Managementsystem

  PLAN – DO – CHECK – ACT

  Damit höherer Reifegrad des Datenschutzprozesses notwendig (Statt CMM Stufe1 CMM Stufe 4-5)

- Statt wie bisher: Rechtsgrundlage und 8 Gebote jetzt
  - Grundprinzipien (Art. 5 DS-GVO)
  - Datenschutzziele (Art. 32 DS-GVO)

activeMind.AG

Klaus Foitzick

Vorstand

Potsdamer Str. 3, 80802 München
Kurfürstendamm 56, 10707 Berlin

foitzick@activemind.de

089 418 560 170

www.activemind.de

- Rechtsanwalt, Bankkaufmann
- Microsoft Certified System Engineer (MCSE)
- VMware Certified Professional (VCP)
- Zertifizierter Audit-Teamleiter für Audits auf der Basis von IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (Zertifizierungsnummer 0066-2017)
- Berufener Auditor des TÜV Hessen ISO 9001 und ISO 27001
- ITIL v3 Manager
- Dozent der IHK Akademie München für Datenschutz, Datensicherheit und Qualitätsmanagement
- Akkreditierter Prüfstellenleiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD)
- Zertifizierter Datenschutzauditor (DSZ)

activeMind.AG

Vielen Dank für die Aufmerksamkeit!

IHK München und Oberbayern