KDO
IT für Kommunen

Datenschutzgrund-verordnung

Torsten Knöller

21. Januar 2019

Alles neu machte der Mai …2018

EU DSGVO: Ziele

- Stärkung des **Grundrechts** auf informationelle Selbstbestimmung des Einzelnen
- Einhaltung europäischer **Datenschutzregelungen auch für Unternehmen außerhalb der EU**
- Höherer Grad an **Harmonisierung und Vereinheitlichung** innerhalb der 28 EU-Mitgliedstaaten zur Schaffung gleicher Wettbewerbsbedingungen
- Modernisierung des Datenschutzrechts unter dem Aspekt zunehmender **Digitalisierung**
- Bildung eines **Datenschutzstandards**

Artikel 1 Abs. 2 Gegenstand und Ziele:

*„Die Verordnung schützt die **Grundrechte und Grundfreiheiten** natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.“*

EU-DSGVO: Regelungen

- **Datenschutz-Grundverordnung = <u>Verordnung</u> (EU) 2016/679**
  - Gilt unmittelbar
  - Verpflichtend ab 25. Mai 2018
  - **Öffnungsklauseln** (Art. 6 Abs. 2) sollen den Mitgliedstaaten die Möglichkeit geben, nationale Regelungen einzubinden, z. B.
    - Art. 83 Verhängung vom Geldbußen -> § 41 Abs. 2 BDSG (nicht für öffentliche Stellen)

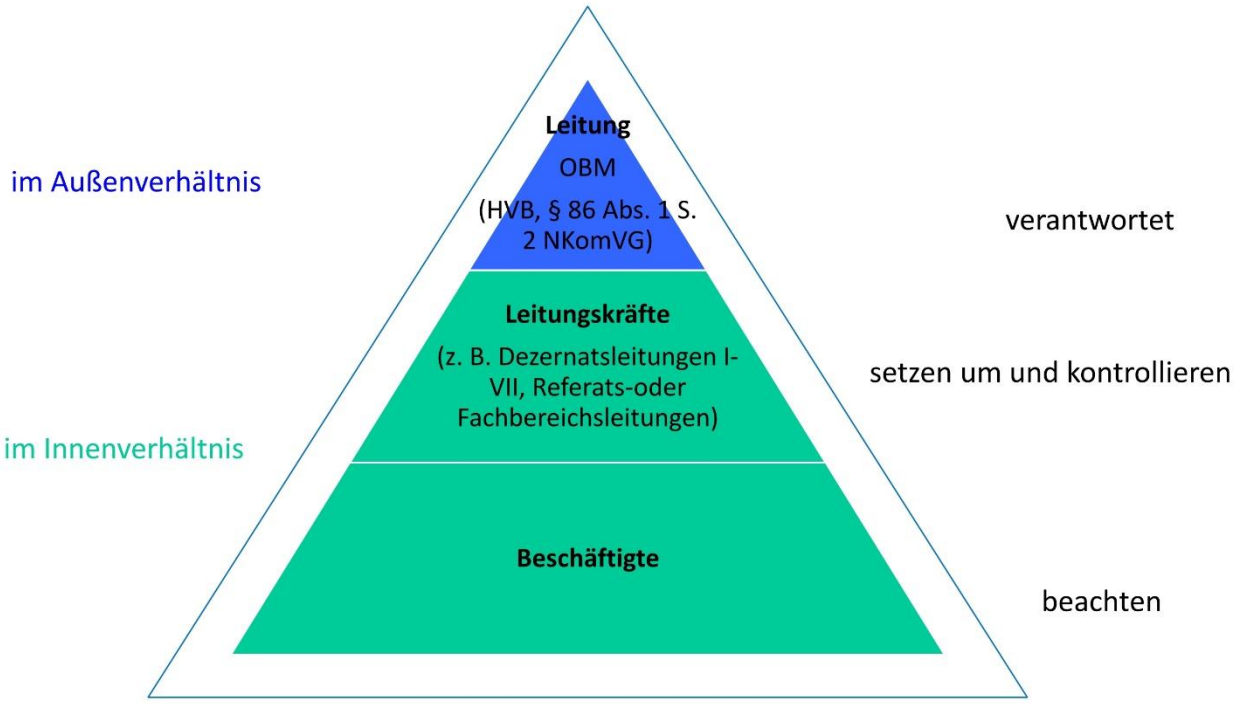
- **Datenschutz-Anpassungs- und -Umsetzungsgesetz EU–DSAnpUG-EU**
  - Am 27. April 17 vom Bundestag verabschiedet – inzwischen vom Bundesrat zugestimmt
  - Neufassung des BDSG (Geltungsbereich: öffentliche Stellen des Bundes und der Länder (soweit keine Landesrechtlichen Regelungen greifen) sowie für nicht-öffentliche Stellen)

- **Landesdatenschutzgesetze und die Datenschutzverordnung**
  - BDSG neu: Veröffentlicht am 5. Juli 2017; trat am 25. Mai 2018 in Kraft!

EU-DSGVO: Anzuwendendes Recht

EU-DSGVO: Verantwortliche

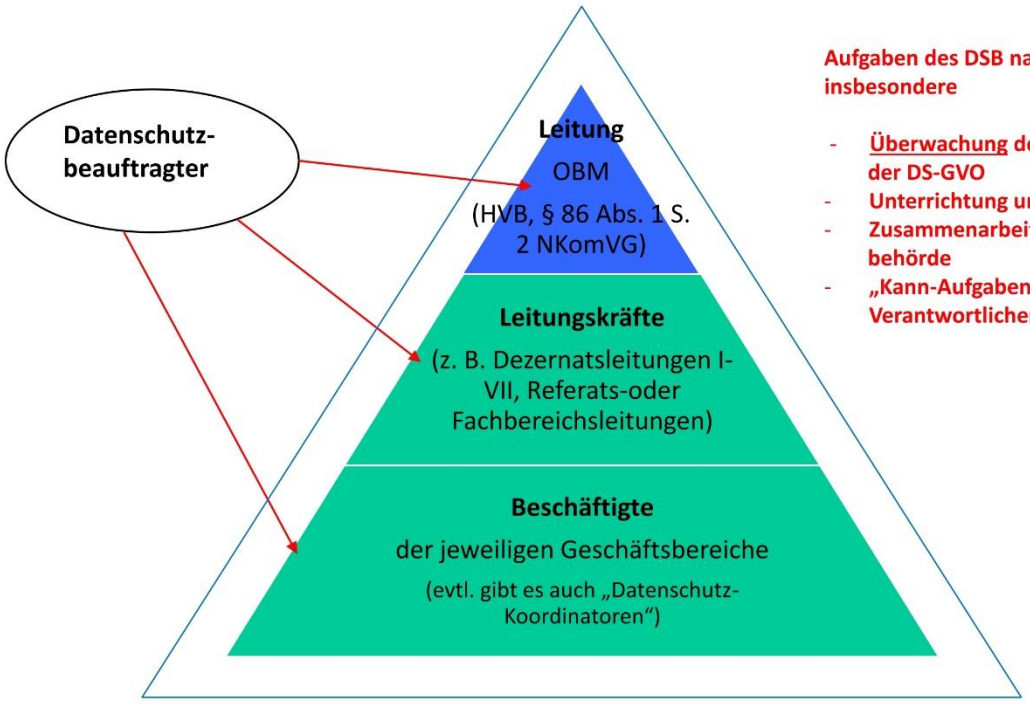
Verantwortlicher



Die Landesbeauftragte für den Datenschutz Niedersachsen

EU-DSGVO: Datenschutzbeauftragter

Rolle Datenschutzbeauftragte/r (DSB)



Aufgaben des DSB nach Art. 39 DS-GVO insbesondere

- Überwachung der Einhaltung der DS-GVO
- Unterrichtung und Beratung
- Zusammenarbeit mit Aufsichts-behörde
- „Kann-Aufgaben“ (Delegation durch Verantwortlichen)

Die Landesbeauftragte für den Datenschutz Niedersachsen

Besondere Regelungen

- Grundsätze für Datenverarbeitung
- Privacy by Design und Privacy by Default
- Auftragsdatenverarbeitung
- Meldungen von Datenschutzverletzungen
- Datenschutz-Folgenabschätzung
- Benennung eines Datenschutzbeauftragten
- Verwendung von Bildern
- Befugnisse der Aufsichtsbehörden und Sanktionen

EU DSGVO: Besondere Regelungen (1)

Grundsätze für die Datenverarbeitung (Kapitel II)

- Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten:
  - Rechtmäßigkeit, Transparenz, Treu und Glauben,
  - Zweckbindung, Datenminimierung, Richtigkeit,
  - Speicherbegrenzung (Löschung), Integrität,
  - Rechenschaftspflicht

- Art. 6 Rechtmäßigkeit der Verarbeitung:
  - Nach Einwilligung, Vorliegen einer ges. Grundlage, Lebensgefahr besteht, Wahrung von berechtigten Interessen

- Art. 7+8 Bedingungen für die Einwilligung
  - Nachweis der verantwortlichen Stelle muss vorliegen, Sachverhalt klar dargestellt werden, Recht auf Widerruf, Sonderstellung für Kinder

- Art. 9 besondere Kategorien pb-Daten
  - Grundsätzlich untersagt, Ausnahmen in Abs. 2 definiert

EU DSGVO: Besondere Regelungen (2)

Artikel 25: Privacy by design – Privacy by default

- Datenschutz durch Technik (privacy by design)

„Der Verantwortliche trifft unter Berücksichtigung des Stands der Technik …. sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen.“

- Datenschutz durch Voreinstellungen (privacy by default)

„Der Verantwortliche trifft durch Voreinstellung geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.“

EU DSGVO: Besondere Regelungen (3)

Artikel 28: Auftragsverarbeiter

- Bei Beauftragung eines Dritten im Auftrage muss dieser Garantien und TOMs nachweisen, dass die Verarbeitung im Einklang mit den Datenschutzanforderungen der DSGVO erfolgt
- Einen schriftlichen Vertrag eingehen
- Muster unter:

  http://www.lfd.niedersachsen.de/themen/auftragsdatenverarbeitung/auftragsverarbeitung-nach-art-28-ds-gvo-161994.html

EU DSGVO: Besondere Regelungen (3)

Artikel 28: Auftragsverarbeiter

- Der Auftragsverarbeiter muss, namentlich nach seinem Fachwissen, seiner Zuverlässigkeit und seinen verfügbaren Ressourcen, dafür **bürgen**, dass die Verarbeitung aufgrund geeigneter technischer und organisatorischer Maßnahmen die **Anforderungen der DS-GVO** einhält und den **Schutz der Rechte** der betroffenen Personen gewährleistet.

- Der Verantwortliche muss sich **fortlaufend** vergewissern, ob der Auftragsverarbeiter die gestellten Anforderungen erfüllt. Es handelt sich dabei um eine Dauerpflicht.

- Liegen die hinreichenden Garantien nicht mehr vor oder zeigt sich erst nach Begründung des Auftragsverhältnisses, dass der Auftragsverarbeiter die erforderlichen Garantien nicht bietet, darf er mit dem Auftragsverarbeiter **nicht mehr zusammenarbeiten**.

EU DSGVO: Besondere Regelungen (4)

Artikel 33: Meldungen von Datenschutzverletzungen

- Datenschutzverletzungen müssen innerhalb von 72 Std. der zust. Aufsichtsbehörde gemeldet werden, wenn ein Risiko für die Betroffenen vorliegt!
- Die **Meldung** enthält **Informationen** über Art der Verletzung, Kategorien der Daten, Anzahl betroffene Personen und Datensätze, Kontaktdaten des Datenschutzbeauftragten, Beschreibung der Folgen der Verletzung des Schutzes personenbezogener Daten sowie **Maßnahmen zur Behebung des Vorfalls**
- Eine vollständige **Dokumentation des Vorfalls** einschließlich der durchgeführten Schritte ist notwendig.

EU DSGVO: Besondere Regelungen (5)

Artikel 35: Datenschutz-Folgenabschätzung

- Durchführung **vor** Inbetriebnahme der Verarbeitung als Nachweis zur Einhaltung der DSGVO!
- Eine Datenschutz-Folgenabschätzung ist durchzuführen, wenn
  - ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht,
  - sensible Daten gemäß Art. 9 Abs. 1 oder Art. 10 verarbeitet werden sollen oder
  - öffentlich zugängliche Bereiche überwacht werden sollen (**Videoüberwachung**).
- Inhalte der Datenschutz-Folgenabschätzung:
  - **Beschreibung** der Verarbeitungsvorgänge,
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge auf den **Zweck** und, die Risiken für die Rechte und Freiheiten der Betroffenen,
  - **Abhilfemaßnahmen** einschließlich Garantien sowie Sicherheitsvorkehrungen und Verfahren

EU DSGVO: Besondere Regelungen (6)

§ 37 BDSG (neu):

Benennung eines Datenschutzbeauftragten

- Ergänzend zu Artikel 37 Abs. 1 DS-GVO benennen der Verantwortliche und der Auftragsverarbeiter einen Datenschutzbeauftragten, soweit **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.
  - Hierzu zählen u.a.:
    - Mitarbeiter
    - Ehrenamtliche
    - Übungsleitende
    - Lehrkräfte

    die personenbezogene Daten regelmäßig verarbeiten.

EU DSGVO: Besondere Regelungen (7)

Verwendung von Bildern

- Kunsturheberrechtsgesetz stützt sich auf eine Vorschrift der DS-GVO (Art. 85 Abs. 1), und fügt sich als Teil der deutschen Anpassungsgesetzgebung in das System der DS-GVO ein, daher:
- Zulässigkeit der Veröffentlichung richtet sich weiterhin nach Kunsturheberrechtsgesetzes (KunstUrhG)
- Damit ergeben sich keine wesentlichen Unterschiede zur aktuellen Praxis. Maßgeblich ist in erster Linie, ob bei der jeweiligen Fotoaufnahme eine (oder mehrere) Person(en) im Mittelpunkt stehen, oder ob die Veranstaltung als solche wiedergegeben wird.

EU DSGVO: Besondere Regelungen (7)

Verwendung von Bildern

- die Veröffentlichung kann mit den entsprechenden Ausnahmetatbeständen des KunstUrhG bzw. mit einer Interessenabwägung nach der DS-GVO gerechtfertigt werden. Damit können Fotos von Veranstaltungen, an denen die abgebildeten Personen teilgenommen haben und/oder auf denen sie praktisch nur als Beiwerk zu sehen sind, auch weiterhin ohne Einwilligung auf der Website oder in Printmedien veröffentlicht werden. Bei geschlossenen Veranstaltungen kann über vertragliche Regelungen (z. B. Veranstaltungs-AGB) eine Veröffentlichungsbefugnis begründet werden.
- Die Annahme, dass die DS-GVO dem Anfertigen oder der Veröffentlichung von Fotografien entgegenstehe, ist daher unzutreffend.

EU DSGVO: Besondere Regelungen (8)

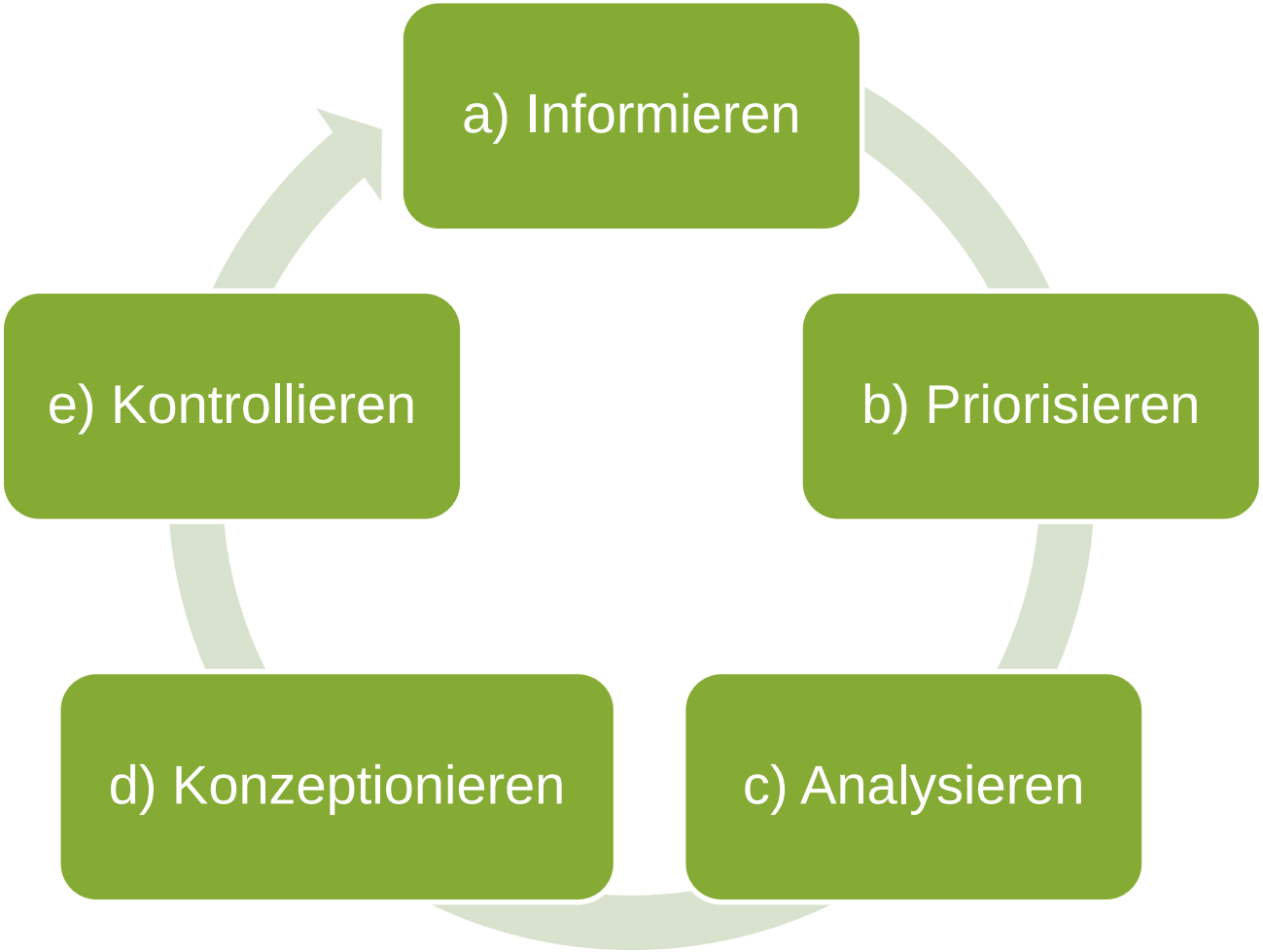
Befugnisse der Aufsichtsbehörden und Sanktionen

- Für Vereine kann nach Art. 83 Abs. 4 ein Bußgeld in Höhe von 10 Mio. oder 2 % des weltweiten Jahresumsatz verhängt werden, wenn gegen die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 - 39, 42 und 43 verstoßen wird.

Worauf muss man sich einstellen?

- Verzeichnis der Verarbeitungstätigkeiten
- Verträge zur Auftragsdatenverarbeitung
- Datenschutz-Folgenabschätzungen
- Leitlinien, Datenschutzkonzepte, Datenschutzrichtlinien
- IT-Sicherheitskonzept mit Beschreibung der getroffenen techn.-org. Maßnahmen
- Dokumentation von Einwilligungserklärungen
- Ggf. Zertifikat/Datenschutzaudit eines unabhängigen Dritten

Wie kann man (pragmatisch) anfangen?



Schritt 1: Informieren

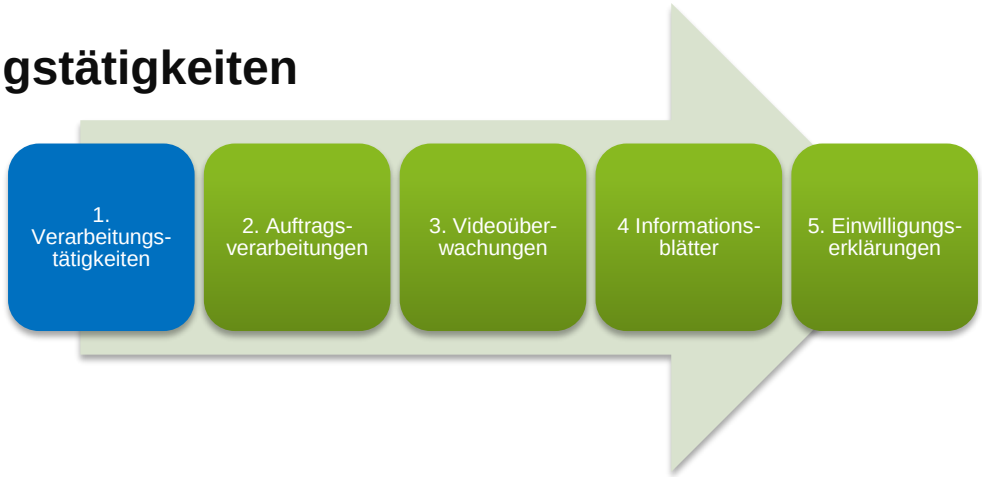
- Über Aufgaben und Auswirkungen der EU-DSGVO informieren
  - Vereinsleitung
  - Mitarbeiter (sofern vorhanden)
- Arbeitsgruppe „EU-DSGVO“ bilden
  - Erstellung eines Aufgabenplans
  - Behandlung wichtiger Themen und Abstimmung hierüber
    - Test zur Selbsteinschätzung: www.lda.bayern.de/dsgvo
- Parallel Datenschutzteam aufbauen
  - Regelmäßiger Austausch
  - Z. B. bestehend aus Vorsitzenden, Webseitenverantwortlichen, Pressewart, …

Schritt 2: **Priorisieren**

- Was sollte ich vorrangig angehen?
- Prioritäten-Liste erstellen, z. B.
  - Webseiten anpassen
    - Datenschutzerklärung, Formulare, Impressum, SSL-Verschlüsselung usw.
  - Kontaktdaten des DSB veröffentlichen sofern erforderlich (Leicht von außen überprüfbar!)
  - Auskunftsanspruch des Betroffenen (Art. 15 EU-DSGVO)
    - Wie gehe ich mit solchen Anfragen um? (Prozess initiieren!)
    - Antwort muss innerhalb eines Monats erfolgen.

Schritt 3: Analysieren / Bestandsaufnahme

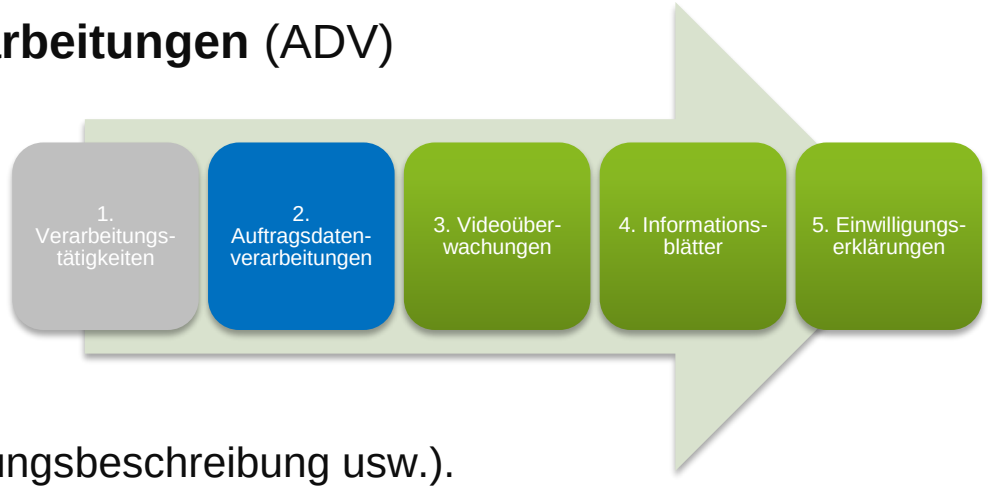
- Punkt 1: Liste der **Verarbeitungstätigkeiten**
- Tool: MS Excel o.ä.



- Aktuelle Liste der relevanten Verfahren erstellen
- Verfahrensbeschreibung(en)

Schritt 3: Analysieren / Bestandsaufnahme

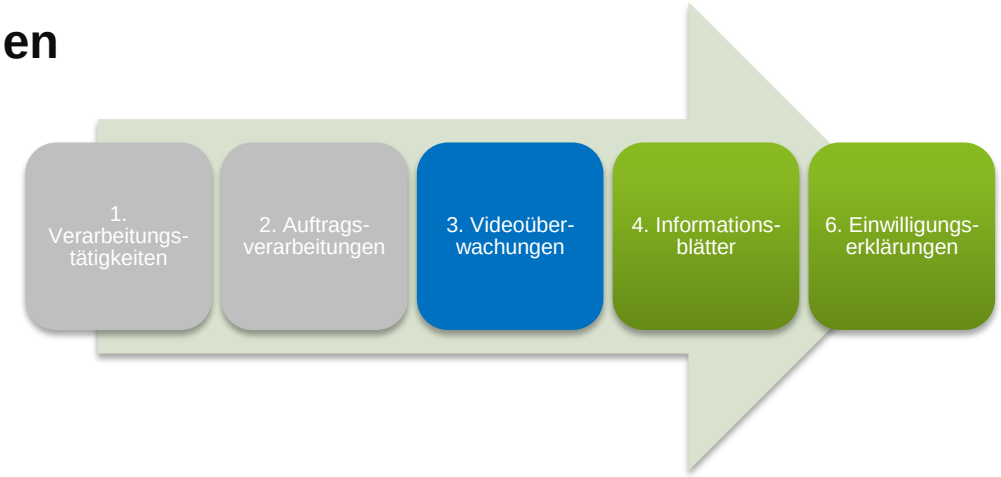
- Punkt 2: **Auftrags(daten)verarbeitungen** (ADV)
- Tool: MS Excel o.ä.
- Was ist ADV?



  - Verträge hierzu prüfen (Leistungsbeschreibung usw.).
  - Erfassung der Daten (Excel).

Schritt 3: Analysieren / Bestandsaufnahme

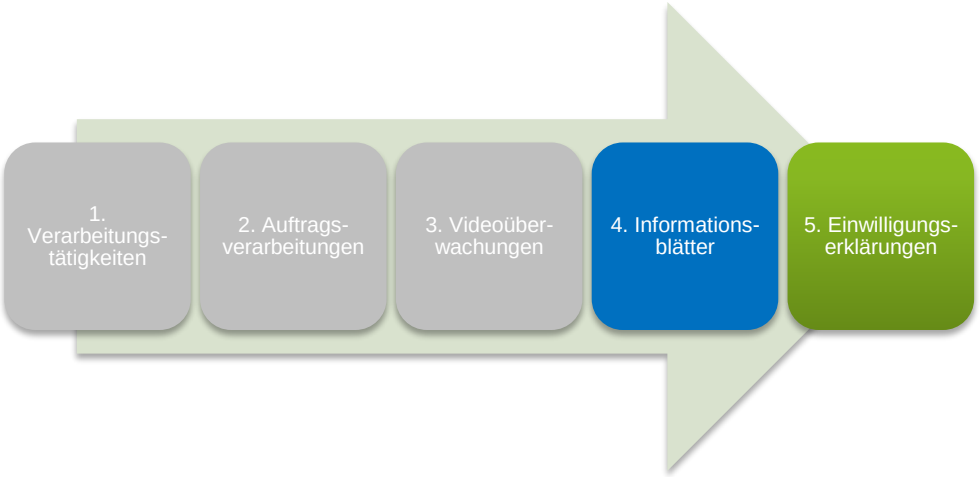
- Punkt 3: **Videoüberwachungen**
- Tool: MS Excel o.ä.



- Findet Videoüberwachung statt?.
- Erfassung der Daten (Excel).
- Prüfen, ob noch erforderlich; wenn ja, Technikfolgenabschätzung durchführen

Schritt 3: Analysieren / Bestandsaufnahme

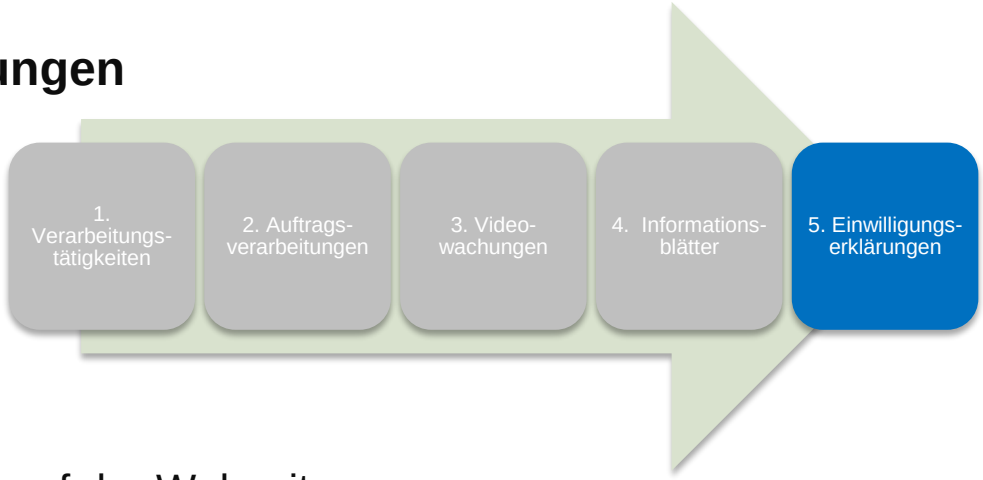
- Punkt 4: **Informationsblätter**
- Tool: MS Excel o.ä.



- Beispiel:
  - Aufnahmeantrag
- Aufgabe:
  - Prüfen, ob alle Informationen gem. Art. 13 und 14 DS-GVO enthalten sind

Schritt 3: Analysieren / Bestandsaufnahme

- Punkt 5: **Einwilligungserklärungen**
- Tool: MS Excel



- Beispiele:
  - Daten von Vereinskameraden auf der Webseite
  - Verwendung von Fotos auf der Webseite

- Zweck benennen, Freiwilligkeit, Möglichkeit des Widerrufs

Schritt 4: Konzeptionieren

- Beschreibung der Verarbeitungstätigkeiten
- Auftragsverarbeitungsverträge
- IT-Konzepte
  - IT-Sicherheit allgemein
  - Patch Management
  - Virenschutz
  - (…)
- Berechtigungs-/Rollenkonzepte
- Schulungskonzept
- (…)

Schritt 5: Kontrollieren

- Überwachung ist eine wesentliche Aufgabe des behördlichen/betrieblichen Datenschutzbeauftragten
- Siehe Aufgabenkatalog (Art. 39 EU-DSGVO).
- Art. 39 (1) Nr. b) EU-DSGVO:

  „Überwachung der Einhaltung der EU-DSGVO, anderer Datenschutzvorschriften sowie der Strategien des Verantwortlichen und des Auftragsverarbeiters (…)“

- … bei Abweichungen Anpassungen vornehmen und (auch) diese dokumentieren!
- Wenn kein DSB benannt werden muss, stellt der Verantwortliche dieses sicher!

Welche Frage darf ich Ihnen beantworten?

Ihre Ansprechpartner

Thorsten Roßkamp

Torsten Knöller

Christofer Fleischhauer

Thorsten Früchtnicht

Martin Jacob

Nils Körner

Theres Meyer

Marcel Grubert

Kontakt
Tel. 0441 9714-158, -159, -180, -2199, -156, -295, -1370, -1316
datenschutz@kdo.de

Zweckverband Kommunale Datenverarbeitung Oldenburg (KDO)
Elsässer Straße 66, 26121 Oldenburg