Österreichischer Städtebund

Die Datenschutzgrundverordnung (DSGVO)

- Eine Herausforderung für die kommunale Verwaltung

Fachausschuss für Kontrollamtsangelegenheiten
24.05.2018

Dr. Johannes Schmid

Österreichischer Städtebund

Etwas provokant formuliert:

Es bleibt alles gleich.

Österreichischer Städtebund

Neues Datenschutzrecht – was bleibt gleich?

Im Wesentlichen: Die Zulässigkeitsprüfung

Was bleibt gleich?

Österreichischer Städtebund

Warum ist dann der Datenschutz in aller Munde?

1. Sanktionen
2. Bisheriger Umgang, bisherige Sensibilisierung

Exkurs: Geldbuße

Österreichischer Städtebund

Drakonische Erhöhung ist mittlerweile bekannt

- Bis EUR 10 Millionen (oder 2 % des Jahresumsatzes)
  - (u.a.)
    - Keine Benennung eines Datenschutzbeauftragter
    - Kein oder ungenügendes Verarbeitungsverzeichnis
- Bis EUR 20 Millionen (oder 4 % des Jahresumsatzes)
  - (u.a.)
    - Verstöße gegen Rechte des Betroffenen, Geheimhaltung, Auskunft, Richtigstellung, Löschung
- Gegen Behörden / öffentliche Stellen:
  - Ausnahmemöglichkeit im nationalen Gesetz:
  - **Davon wurde im DSG Gebrauch gemacht (§ 30 Abs 5 DSG)**
  - **→ keine Geldbußen für Behörden und öffentliche Stellen.**

Exkurs: Geldbuße

Drakonische Erhöhung ist mittlerweile bekannt

VORSICHT BEIM FREIBRIEF:

Fraglich, ob der Entfall der Geldbuße nur für die Hoheitsverwaltung gilt!?

Umkehrschluss: Fraglich, ob die Gemeinde für privatwirtschaftliches Handeln (doch) bestraft werden kann

arg dafür: VfGH-Judikatur (zB VfSlg. 19.988/2015)

arg dagegen: Klarer Wortlaut der DS-GVO und des DSG

→ Anfrage an die Datenschutzbehörde bringt auch keine Klarheit

(*„Die Frage, ob durch privatwirtschaftliches Handeln einer öffentlichen Stelle das Privileg nach § 30 Abs 5 DSG wegfällt, wird erst durch die Rechtsprechung zu klären sein.“*)

Exkurs: Geldbuße

- **Was gerne vergessen wird …**
  - **Datenschutzbehörde** erhält Strafbefugnis
    - Ankläger und Richter
    - Bisher Bezirksverwaltungsbehörde
  - **Sonstige** Sanktionen
    - Politische Konsequenzen
    - Reputation
    - Schadenersatz
    - Unterlassung
    - Verfahrenskosten (Beschwerde an die Behörde; Klage bei den ordentlichen Gerichten)

Die Zulässigkeitsprüfung

Dennoch vermehrt Frage: „*Darf ich das?*“

Antwort: Zulässigkeitsprüfung

→ Verbotsprinzip

Alles ist verboten, außer es ist erlaubt

Was ist erlaubt?

1. Gibt es einen **Rechtfertigungsgrund**?
2. Sind die **datenschutzrechtlichen Grundsätze** eingehalten?

Was bleibt gleich?

Zulässigkeitsprüfung: Wann ist eine Datenverarbeitung zulässig?

1. Rechtmäßige Datenverarbeitung

Prüfung, ob Rechtfertigungsgründe erfüllt sind

Unterschied: Sensible <--> nicht sensible Daten (*„Daten besonderer Kategorien“*)

2. Datenschutzrechtliche Grundsätze

Rechenschaftspflicht

Zweckbindung

Verhältnismäßigkeit

Datenminimierung

Transparenz

Fair und nach Treu und Glauben

Speicherbegrenzung

Was bleibt gleich?

1. Rechtfertigungsgründe

„Nicht-sensible“ Daten

(auszugsweise)

- Einwilligung
- Notwendigkeit zur Vertragserfüllung / vorvertragliche Maßnahmen auf Anfrage
- Rechtliche Verpflichtung (aus einem Gesetz)
- Übertragene Aufgabe im öffentlichen Interesse oder mit hoheitlicher Gewalt
- Lebenswichtige Interessen (des Betroffenen oder eines Dritten)

- Überwiegende Interesse des Verantwortlichen oder eines Dritten
  - = Interessensabwägung
  - Im hoheitlichen Bereich nicht zulässig!?

Was bleibt gleich?

1. Rechtfertigungsgründe

„*Sensible*“ Daten (*Daten besonderer Kategorien* inkl strafrechtsrelevanter Daten)

(auszugsweise)

- Ausdrückliche Einwilligung
- Ausübung von Rechten / Erfüllung von Pflichten aus dem Arbeitsrecht
- Verpflichtung aus gesetzlicher Vorschrift und öffentliches Interesse
- Geltendmachung / Verteidigung von Rechtsansprüchen
- Lebenswichtige Interessen des Betroffenen (und mangelnde Einwilligungsfähigkeit)
- Vom Betroffenen veröffentlichte Daten

Was bleibt gleich?

2. Datenschutzrechtliche Grundsätze

Zweckbindung

Zweckänderung:

- Neuer Zweck mit altem Zweck vereinbar → keine neue Rechtfertigung, also zb keine neue Zustimmung

(aber Informationspflicht)

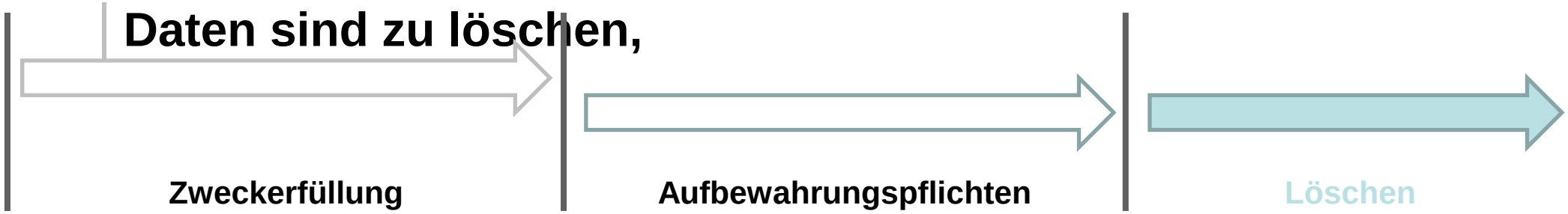
- Nicht vereinbar: Neue Rechtsgrundlage

Was bleibt gleich?

2. Datenschutzrechtliche Grundsätze

Zweckbindung

Daten sind zu löschen,



wenn sie für den Zweck nicht mehr erforderlich sind und keine Aufbewahrungspflicht besteht

Was bleibt gleich?

Exkurs Aufbewahrungsfristen

- 6 Monate
  - Bewerberdaten; 6 Monate gerechnet ab erfolgloser Bewerbung
  - Ausnahme: Zustimmung für längere Aufbewahrung
- 7 Jahre
  - Bücher und Belege; § 132 BAO; UGB
- 10 Jahre
  - Dokumentationen im Gesundheitsbereich
  - Unterlagen für allfällige Ansprüche aus der Produkthaftung
- 22 Jahre
  - Grundstücksgeschäfte; UStG
- 30 Jahre
  - Daten, die zur Erstellung von Dienstzeugnissen notwendig sind
  - Daten über Arbeitsunfälle (allg. absolute Verjährungsfrist für Schadenersatzansprüche)

Was bleibt gleich?

2. Datenschutzrechtliche Grundsätze

Verhältnismäßigkeit / Datenminimierung / Speicherbegrenzung

- Daten dürfen nur dem Zweck entsprechend angemessen und im (bloß) beschränkten Maß verarbeitet werden
- zB: Zweck auch mit anonymisierten Daten erreichbar (zB Statistik) → überschießende Datenverarbeitung
- zB: Speicherung aller Download-Parameter, wenn nur das Datenvolumen relevant ist
- Löschpflicht nach Ablauf der Aufbewahrungsfristen

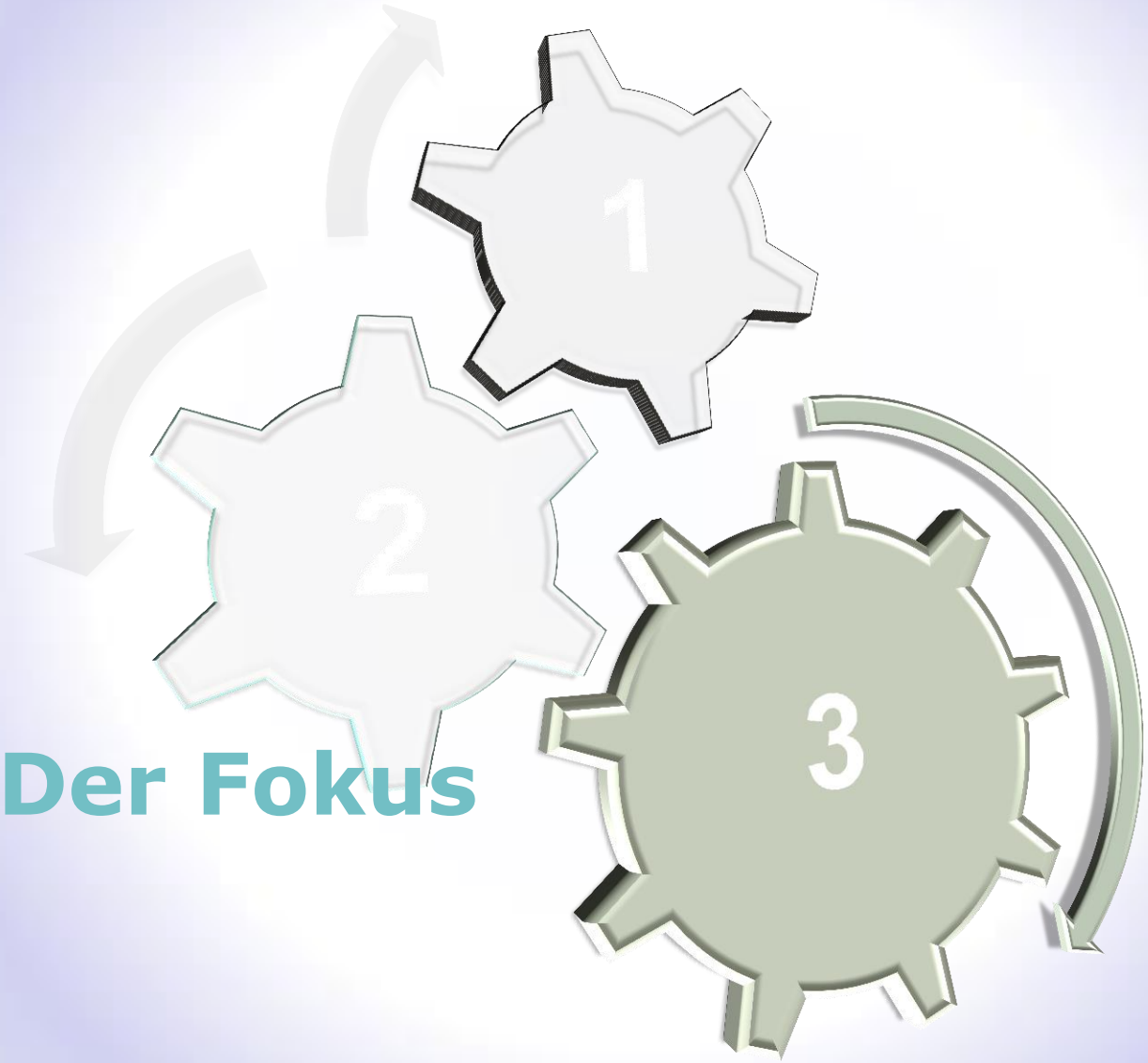
Rechenschaftspflicht

- Grundsätze einhalten
- Einhaltung auch nachweisen zu können
- → Dokumentation (*„Datenschutz-Ordner“*)

Zusammenfassend:

Zulässigkeitsprüfung

(was zulässig ist, bleibt zulässig)



Der Fokus

Was wird neu?

Neues Datenschutzrecht – was wird neu?

- Der bürokratische Aufwand
  - Informationspflichten
  - **Rechenschaftspflicht** (Interne Richtlinien, **Reaktionsprozedere**, Löschkonzept, Nachweise, Amtsvermerke, Protokolle, allgemein: *„Gedanken zum Datenschutz*")
  - → ***„Datenschutz-Ordner*"**
  - technische/organisatorische Maßnahmen zur Datensicherheit
  - **Datenverarbeitungsverzeichnis**
- Pflicht zur Bestellung eines Datenschutzbeauftragten (?)
- Sanktionen

Der Fokus

- **Datenverarbeitungs-Verzeichnis**
  - Zentrale Verpflichtung
  - Ausgangsbasis für alles
  - Erster Kontrollpunkt
- **Reaktion auf Auskunfts- und Löschungsbegehren**
  - Zu erwartende Spitze Mai/Juni bzw Sommer
  - Durch mediale Berichterstattung
  - Potenzielle Verfahren vor der DSB
- **Nach außen gerichtete Handlungen**
  - Angriffsflächen, haftungsträchtig

Der Fokus

- **Datenverarbeitungs-Verzeichnis**
  - Zentrale Verpflichtung
  - Ausgangsbasis für alles
  - Erster Kontrollpunkt
- **Reaktion auf Auskunfts- und Löschungsbegehren**
  - Zu erwartende Spitze Mai/Juni bzw Sommer
  - Durch mediale Berichterstattung
  - Potenzielle Verfahren vor der DSB
- **Nach außen gerichtete Handlungen**
  - Angriffsflächen, haftungsträchtig

Was wird neu?

Datenverarbeitungs-Verzeichnis

- Bisherige Meldepflicht entfällt
- Ersatz: Führung eines Verzeichnisses über alle Datenverarbeitungen

Form

- Schriftlich oder elektronisch ausdruckbar (zB Word, Excel, Datenbank)

Was wird neu?

- **Datenverarbeitungs-Verzeichnis**
- Inhalt
  - Alle Datenverarbeitungen
  - Eine Verarbeitung – ein Eintrag
    - Variante 1: *„Personaldatenverwaltung“*
    - Variante 2: *„Lohnbuchhaltung“*, *„Bewerbungen“*, *„Zeiterfassung“, „Dienstzeugnis“* als eigene Verarbeitungen?
    - Für Verantwortliche wohl einzelne – jedoch nicht zu detaillierte – Betrachtung

      („Kategorien“ sind nur für Auftragsverarbeiter genannt)
  - Mögliche Abgrenzungen
    - Speicherfrist
    - Rechtsgrundlage

Was wird neu?

- **Datenverarbeitungs-Verzeichnis**
- Inhalt
  - Besondere Angaben pro Verarbeitung:
    - Zweck, Art der Daten
    - Welche Betroffenen, welche Empfänger
    - Allfällige Löschfrist (wenn möglich)
  - Allgemeine Angaben
    - Name und Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten
    - Technische und organisatorische Maßnahmen zur Datensicherheit

Was wird neu?

Datenverarbeitungs-Verzeichnis

Ausnahme!?

< 250 Mitarbeiter und

bloß gelegentliche,

risikofreie Verarbeitung

von nicht-sensiblen Daten

→ fraglich, ob überhaupt möglich

zB Foto Mitarbeiter: wird für jeden neuen MA angefertigt (nicht gelegentlich)

Der Fokus

- **Datenverarbeitungs-Verzeichnis**
  - Zentrale Verpflichtung
  - Ausgangsbasis für alles
  - Erster Kontrollpunkt
- **Reaktion auf Auskunfts- und Löschungsbegehren**
  - Zu erwartende Spitze Mai/Juni bzw Sommer
  - Durch mediale Berichterstattung
  - Potenzielle Verfahren vor der DSB
- **Nach außen gerichtete Handlungen**
  - Angriffsflächen, haftungsträchtig

Was ist zu tun?

- **Reaktion auf Anträge von Betroffenen**
  - Recht auf Auskunft
  - Recht auf Richtigstellung
  - Recht auf Löschung
  - Widerspruch

- DSGVO neu:
  - Recht auf Vergessen (werden)
  - Recht auf Datenportabilität

Was ist zu tun?

Reaktion auf Anträge von Betroffenen

Recht auf Auskunft – Umsetzung in der Praxis

Recht auf Löschung

Was ist zu tun?

Umsetzung in der Praxis:

Vorbereitungen

1. Definieren einer zuständigen Stelle
2. Definieren von *„neuralgischen“* Mitarbeiter_innen (Abteilungsleiter, Personalabteilung, IT, etc.)
3. Definieren der gängigsten zu erteilenden Informationen (anhand DVV, etc.)
4. Entwurf eines Muster-Antwortschreibens (für Vorhandensein und Nicht-Vorhandensein von Daten)
5. Sicherstellung, dass Antwort sowohl postalisch als auch elektronisch versendet werden kann

Was ist zu tun?

Umsetzung in der Praxis:

Reaktionsprozedere festlegen (im Falle eines Ersuchens)

1. Unmittelbare Weiterleitung an die zuständige Stelle (unabhängig ob Eingang persönlich/postalisch/elektronisch)
2. Fristvormerk
3. Identitätsfeststellung (unterfertigte Ausweiskopie, telefonische Rückfrage, Aktenvermerk bei pers. Bekanntheit)
4. Zuständige Stelle: Einforderung der Daten (EDV; bei Papier: neuralgische Mitarbeiter_innen)
5. Nach 3 Wochen: Klärung, ob die 1-Monats-Frist ausreicht
6. Innerhalb der 1-Monats-Frist: Erste Beantwortung oder Negativmitteilung oder Fristverlängerung
7. Aufforderung zur Mitwirkung samt Fristsetzung
8. Weitere Recherchen anhand der Rückantwort
9. Ergänzende Beantwortung
10. Dokumentation der erfolgten Beauskunftung

Was ist zu tun?

Reaktion auf Anträge von Betroffenen

- Recht auf Auskunft
- **Recht auf Löschung**

Was bleibt gleich?

Zur Erinnerung:

Was ist zu tun?

Reaktion auf Anträge von Betroffenen

- Recht auf Auskunft
- **Recht auf Löschung – Umsetzung in der Praxis**

Was ist zu tun?

Umsetzung in der Praxis:

Vorbereitungen

1. Definieren einer zuständigen Stelle
2. Definieren von *„neuralgischen"* Mitarbeiter_innen (EDV, bei Papier: Abteilungsleiter, Personalabteilung)
3. Kontaktdaten eines allfälligen externen EDV-Dienstleisters
4. Übersicht aller gängigen Aufbewahrungsfristen
5. Erarbeiten geeigneter Löschregeln (Datenart + Löschfrist + Startzeitpunkt der Löschfrist)
6. Unterscheidung Daten, Archivdaten, Sicherheitskopien, gesperrte Daten
5. Entwurf eines Muster-Informationsschreibens

Was ist zu tun?

Umsetzung in der Praxis:

Löschkonzept festlegen

1. Unmittelbare Weiterleitung an die zuständige Stelle (unabhängig ob Eingang persönlich/postalisch/elektronisch)
2. Fristvormerk
3. Identitätsfeststellung (unterfertigte Ausweiskopie, telefonische Rückfrage, Aktenvermerk bei pers. Bekanntheit)
4. Zuständige Stelle: interner Löschauftrag (EDV; bei Papier: neuralgische Mitarbeiter_innen)
5. Einforderung der Bestätigungen
6. Nach 3 Wochen: Klärung, ob die 1-Monats-Frist ausreicht
7. Innerhalb der 1-Monats-Frist: Informationsschreiben versenden oder Fristverlängerung
8. Aufforderung zur Mitwirkung samt Fristsetzung
9. Weitere Löschungen anhand der Rückantwort
10. Dokumentation der erfolgten Löschung

Der Fokus

- **Datenverarbeitungs-Verzeichnis**
  - Zentrale Verpflichtung
  - Ausgangsbasis für alles
  - Erster Kontrollpunkt
- **Reaktion auf Auskunfts- und Löschungsbegehren**
  - Zu erwartende Spitze Mai/Juni bzw Sommer
  - Durch mediale Berichterstattung
  - Potenzielle Verfahren vor der DSB
- **Nach außen gerichtete Handlungen**
  - Angriffsflächen, haftungsträchtig

Was ist zu tun?

Rechtskonforme Ausgestaltung von

- Homepage
  - **Datenschutzerklärung**
  - Cookies, tracking tools
- Newsletter / Zusendungen / Werbung
- Einwilligungserklärungen
- Videoüberwachung

Was ist zu tun?

> **Davon ausgewählt:**
>
> > Wie hole ich eine wirksame Einwilligung ein?

Ausgewählte Fragen

- **Einwilligung**
  - Anforderungen wie bisher
    - Freiwillig und in Kenntnis der Sachlage
- Neu: Klarstellungen
  - Koppelungsverbot
    - Keine freiwillige Einwilligung, wenn davon die Erfüllung des Vertrages bzw Vertragsabschluss abhängig ist
  - Aktives Handeln
    - Erklärung oder eindeutige bestätigende Handlung
    - Nicht: Stillschweigen, bereits angekreuzte Checkboxen
  - Widerrufsmöglichkeit (und: Hinweis darauf!)
    - Folge: Einwilligung kein Rechtfertigungsgrund mehr; andere Gründe aber denkbar

Ausgewählte Fragen

Einwilligung

Einwilligungen bereits jetzt umstellen

- Mitarbeiter, Kunden, Vertragspartner
- Aktuelle Einwilligungen bleiben zulässig, wenn sie inhaltlich und formell den Anforderungen der DSGVO entsprechen

Musterformulierung

> *„Hiermit erteile ich meine ausdrückliche Zustimmung, dass meine personenbezogenen Daten, nämlich <Auflistung>, von <Verantwortlicher> zum Zwecke* ***<Auflistung der Zwecke der Datenverarbeitungen>*** *gespeichert, verarbeitet und an <Liste der Empfänger> übermittelt werden. Diese Zustimmung kann jederzeit per E-Mail an <E-Mail-Adresse> widerrufen werden.“*

Datenschutzbeauftragter

Pflicht zur Bestellung eines Datenschutzbeauftragten

Verpflichtend für

- für Behörden oder andere öffentliche Stellen
- Unternehmen, deren Kerntätigkeit
  - die umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht oder

(Kreditauskunfteien, Banken, Versicherungen, Bewertungsplattformen, IT-Dienstleister)

  - in der umfangreichen Verarbeitung sensibler oder strafrechtlich relevanter Daten liegt

(Krankenhausträger; nicht: einzelne Personen, zB Arzt, Strafverteidiger, weil nicht „umfangreich“)

- Weitere Möglichkeiten durch nationalen Gesetzgeber nicht ausgeschöpft
  - Insbesondere Abgrenzung auf Größe des Unternehmens, etc.

Datenschutzbeauftragter

Pflicht zur Bestellung eines Datenschutzbeauftragten

→ *„Eigene“* Unternehmen von Gebietskörperschaften?

Nicht definiert in der DSGVO

Nicht alle öffentlichen Unternehmungen müssen einen Datenschutzbeauftragten bestellen

Lehrmeinung 1:

Anlehnen an das Vergaberecht: **Öffentliche Stelle dann, wenn**

- im Allgemeininteresse liegende Aufgaben nicht gewerblicher Art verrichtet werden und
- Finanzierung oder Leitung/Kontrolle durch die Gebietskörperschaft gegeben ist

→ Ausschreibungspflichtig = Pflicht zur Bestellung eines DS-Beauftragten

Lehrmeinung 2:

Entscheidend ist Art der Tätigkeit

(schlichte) Hoheitsverwaltung = Pflicht zur Bestellung eines DS-Beauftragten.

Zusammenfassend:

Verzeichnis
Auskunft-/Löschung
Angriffsflächen

DS-Beauftragter?

Sensibilisierung
Zweckbindung

Zulässigkeitsprüfung
(was zulässig ist, bleibt zulässig)

Verzeichnis
Auskunft-/Löschung
Angriffsflächen
DS-Beauftragter?

Österreichischer Städtebund

Die Datenschutzgrundverordnung (DSGVO)

- Keine Herausforderung für die kommunale Verwaltung

Viel Glück !!

Fachausschuss für Statistik
04.05.2018
Dr. Johannes Schmid