# 1. Fragen und Antworten zum persönlichen Anwendungsbereich der DSGVO

## ? Frage 1:

Gilt die DSGVO ab 25. 5. 2018 auch für **juristische Personen?**

**Antwort:**

**Nein.**

1. Art 1 (1) DSGVO umschreibt deren persönlichen Anwendungsbereich dahin, dass diese **nur** Vorschriften zum Schutz **natürlicher Personen** bei der Verarbeitung personenbezogener Daten enthält. Zudem werden in Art 4 (1) DSGVO „personenbezogene" Daten ausdrücklich als „alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche Person**" beziehen, definiert.

2. Die ab 25. 5. 2018 geltende Fassung des DSG enthält in § 1 (1) zwar weiterhin eine Formulierung des **Grundrechts auf Datenschutz,** die von **„Jedermann"** als Grundrechtsbegünstigten spricht, worunter der Verfassungsgerichtshof bisher auch juristische Personen verstanden hat. In § 4 (1) DSG werden aber der innerstaatliche sachliche **Anwendungsbereich** der DSGVO und des DSG auf die **Verarbeitung** personenbezogener Daten **natürlicher Personen** eingeschränkt.

3. Vom Ausschluss der Anwendbarkeit der DSGVO bzw der einfachgesetzlichen Durchführungsbestimmungen hierzu (§§ 5 ff DSG) auf juristische Personen zu unterscheiden ist die Frage der **Reichweite** des **Datenschutzgrundrechts.** Letzteres ist Ausfluss des nationalen Verfassungsrechts und nicht durch die DSGVO vorherbestimmt. Solange der Verfassungsgesetzgeber das Grundrecht nicht ausdrücklich auf natürliche Personen beschränkt, wie dies noch im Entwurf für das Datenschutz-Anpassungsgesetz 2018 vorgesehen war, ist insofern davon auszugehen, dass sich juristische Personen weiterhin zumindest auf das (Teil-)Datenschutzgrundrecht auf **Geheimhaltung** berufen können. Die Möglichkeit der Anrufung der Datenschutzbehörde wegen einer Verletzung dieses Rechts ist juristischen Personen aber durch das DSG nicht eingeräumt. **Praktische Bedeutung** kann dem genannten Recht aus Sicht juristischer Personen am ehesten im Kontext einer Beschwerde gegen überschießende staatliche Ermittlungen (vgl § 106 StPO) oder in einem Normenkontrollverfahren vor dem Verfassungsgerichtshof (vgl § 140 [1] lit c] und d] und Art 144 [1] B-VG) zukommen.

4. Die übrigen Teilgrundrechte (Auskunft, Richtigstellung und Löschung) stehen unter einem Ausgestaltungsvorbehalt. Infolge des Entfalls der nach dem DSG 2000 noch auf juristische Personen anwendbaren Ausführungsbestimmungen können sich juristische Personen auf die vorgenannten Teilgrundrechte nicht mehr berufen (vgl DSB 19. 7. 2018, DSB-D123.089/0002-DSB/2018).

5. ! Mittelfristig ist zu erwarten, dass die Reichweite des Datenschutzgrundrechtes ausdrücklich auf natürliche Personen eingeschränkt wird. Selbst dann verbliebe juristischen Personen aber noch der durch die Verfassungsbestimmung des Art 8 EMRK gewährte Schutz auf Privatsphäre.

## ? Frage 2:

Welche praktischen **Konsequenzen** hat der **Ausschluss juristischer Personen** aus dem **Anwendungsbereich** der **DSGVO** bzw der diese durchführenden DSG-Bestimmungen? Was bedeutet dieser insbesondere für den **Umgang mit Kontaktdaten** der Vertreter der juristischen Person?

**Antwort:**

1. Für die Verarbeitung aller **Daten über eine juristische Person ,** die **nicht** zugleich **auf** deren **Mitarbeiter** oder deren **Führungspersonal bezogen** sind (Bsp: Bezug bestimmter Waren oder Dienstleistungen, Bonitätsdaten, Adressdaten, Zuordnung zu einem Geschäftszweig etc), bedarf es keinerlei datenschutzspezifischer Vorkehrungen. Es bedarf somit weder einer Aufnahme derartiger Verarbeitungen in das Verzeichnis der Verarbeitungstätigkeiten nach Art 30 (2) DSGVO, noch Informationsmaßnahmen iS von Art 12 ff DSGVO und auch keiner organisatorischer Maßnahmen zur Handhabung von Auskunftsersuchen iS von Art 15 DSGVO etc.

2.1. Die **Verarbeitung von Kontaktdaten** von Mitarbeitern bzw von Leitungsorganen einer juristischen Person (Bsp: Kontakte in Mailprogrammen oder spezielle Kontaktdatenbanken), mit der eine andere juristische Person korrespondiert, **unterliegt** dagegen grundsätzlich **der DSGVO** bzw dem **DSG .** Soweit es sich dabei um von der juristischen Person selbst öffentlich gemachte Daten handelt (Bsp: Firmenwebsite) oder sie zwingend in öffentliche Registern aufzunehmen sind (Name, Geburtsdatum und Anschrift vertretungsbefugter Personen; vgl bspw § 3 [1] Z 8, 9 und [2] FBG) fehlte es freilich an einer entsprechenden Schutzwürdigkeit.

2.2. Von der prinzipiellen Qualifikation von Kontaktdaten der Mitarbeiter bzw Vertreter einer juristischen Person als „personenbezogene Daten" iSd Art 4 (1) DSGVO zu unterscheiden ist die Frage der **Zulässigkeit der Verwendung** ebendieser **Kontaktdaten für Werbezusendungen.** Herkömmliche Postsendungen zu Werbezwecken sind bis auf Widerruf möglich (vgl Art 6 [1] lit f], Art 21 [2] und [3] DSGVO iVm § 151 [9] und [11] GewO 1994). Für Werbeanrufe, Werbe-SMS oder Werbe-E-Mails sind die Bestimmungen des § 107 TKG 2003 zu beachten, welche gleichermaßen für natürliche und juristische Personen gelten.

3. Der Ausschluss juristischer Personen als Begünstigte („Betroffene") iSd Art 4 (1) DSGVO ändert nichts an die Bindung solcher juristischer Personen an die DSGVO, wenn es um die **Verarbeitung** der Daten ihrer **Mitarbeiter** oder ihrer **Endkunden** geht. Diesfalls agieren die juristischen Personen selbst als Verantwortliche iSd Art 4 (7) DSGVO.

## ? Frage 3:

Sind **politische Funktionsträger** (einer Gemeinde) **von** der **DSGVO** erfasst? Anders gefragt: Können die Namen von Bürgermeistern in ihrer amtlichen Funktion und unter der Adresse der Gemeinde verarbeitet werden, ohne dass einschlägige Verpflichtungen nach der DSGVO ausgelöst werden (Rechtsgrundlage, Informationsverpflichtung etc)?

**Antwort:**

1. In Bezug auf „politische" Mandatare wird davon auszugehen sein, dass sich deren Wahl bzw Bestellung als Ergebnis eines öffentlichen demokratischen Willensbildungsprozesses

darstellen. Die Identität der Mandatare, deren Funktion sowie deren inhaltliche politische Ausrichtung sind insofern der Öffentlichkeit bekannt und die Zugänglichmachung dieser Informationen im öffentlichen Informationsinteresse gelegen. Für eine Anwendung des Datenschutzgrundrechts auf die genannten Eckdaten bleibt insofern mangels Schutzwürdigkeit bzw wegen allgemeiner Verfügbarkeit kein Raum (vgl § 1 [1] DSG) .

2. Die DSGVO enthält zwar keine dem § 1 (1) DSG vergleichbare Einschränkung des Anwendungsbereiches. Jedoch erscheint logisch erschließbar, dass auch deren Anwendungsbereich dort endet, wo es an der Schutzwürdigkeit der personenbezogenen Daten fehlt. Folgt man dieser Argumentation, finden in Bezug auf die unmittelbar mit der Mandatsausübung verbundenen Daten die Vorgaben der DSGVO zu Rechtsgrundlage und Informationspflichten etc keine Anwendung.

## ? Frage 4:

Ist die **DSGVO für Unternehmen,** die **nur** Business-to-business **(B2B) tätig** sind, überhaupt von **praktischer Relevanz?**

**Antwort:** Ja.

1. Soweit eine juristische Person einem **Einzelunternehmer** und damit einer natürlichen Person gegenübersteht, kann sich Letztere(s) insbesondere auf die Betroffenenrechte nach der DSGVO berufen.
2. S im Übrigen Pkte 2.1 bis 3 der Antwort auf → Frage 1.2, Seite 2.

## ? Frage 5:

Ist die **DSGVO für** als **juristische Personen** eingerichtete Unternehmen, die **nur mit** anderen **juristischen Personen** Geschäfte tätigen, von **praktischer Relevanz?**

**Antwort:**

**Ja,** uzw insofern als **Kontaktdaten** natürlicher Personen sowie Daten eigener Mitarbeiter verarbeitet werden (→ s Pkte 2.1 bis 3 der Antwort auf → Frage 1.2, Seite 2).

## ? Frage 6:

Wie können **Geschäfts- und Betriebsgeheimnisse** von **Unternehmen** geschützt werden, wenn die DSGVO nur für natürliche Personen gilt?

**Antwort:**

1. Einzelne Aspekte von DSGVO-Vorgaben zum Schutz personenbezogener Daten natürlicher Personen haben **indirekte Schutzeffekte** zugunsten Geschäfts- und Betriebsgeheimnissen (vgl bspw Art 5 [1] lit f] und Art 32 [1] lit b] [„Gewährleistung der „Integrität und Vertraulichkeit"]; Art 28 [3] lit b] [„Vertraulichkeitsverpflichtung der Mitarbeiter des Auftragsverarbeiters"]; Art 29 [„Datenverarbeitung durch Mitarbeiter/Auftragsverarbeiter ausschließlich auf Weisung des Verantwortlichen"]; Art 38 [5] [„Verschwiegenheitspflicht des betrieblichen Datenschutzbeauftragten"]; Art 54 [2] [„Amtsverschwiegenheitspflicht der Bediensteten der Aufsichtsbehörde"]).

2. **Auch** die im **DSG** angeordnete gesetzliche **Verschwiegenheitspflicht** für Verantwortliche, Auftragsverarbeiter und deren Mitarbeiter betreffend personenbezogene Daten, die diesen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung mit Datenverarbeitung anvertraut wurden oder zugänglich geworden sind **(„Datengeheimnis"**; § 6 [1]), unterstützt de facto den Schutz von Betriebs- und Geschäftsgeheimnissen. Sinngemäßes gilt für die in § 6 (2) 1 DSG statuierte Pflicht von Verantwortlichem und Auftragsverarbeiter, ihre Mitarbeiter vertraglich zu verpflichten, das Datengeheimnis **auch nach Beendigung** des **Arbeitsverhältnisses** (Dienstverhältnisses) einzuhalten. Auch deren **Belehrungspflicht** gegenüber den Mitarbeitern (§ 6 [3] DSG) über die Grenzen der zulässigen Datenverarbeitung und die **Rechtsfolgen** einer Verletzung des Datengeheimnisses (§ 62 [1] Z 2 DSG; s → Frage 16.3, Seite 78) dient mittelbar dem Schutz von Betriebs- und Geschäftsgeheimnissen. In der Praxis lässt sich die Belehrungspflicht ohne weiteres mit einer **ergänzenden Verpflichtungserklärung** der Mitarbeiter zum Schutz auch von (nicht personenbezogenen) Geschäfts- und Betriebsgeheimnissen verbinden (vgl dazu das Bsp in → Anhang 8, Seite 171). In deren Rahmen kann auch eine **Konventionalstrafe** für den Fall des Bruches der Vertraulichkeit vereinbart werden, welche aber nicht übertrieben hoch sein darf (OGH 25. 9. 1979, 4 Ob 55/79; 24. 6. 2016, 9 Ob A68/16i). Sinngemäßes gilt im Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter.

3.1. Speziell für **Betriebsratsmitglieder** sieht § 115 (4) ArbVG die ausdrückliche Verpflichtung vor, über alle in Ausübung ihres Amtes bekanntgewordenen Geschäfts- und Betriebsgeheimnisse, insbesondere über die ihnen als geheim bezeichneten technischen Einrichtungen, Verfahren und Eigentümlichkeiten des Betriebes Verschwiegenheit zu bewahren. Die Verletzung dieser Pflicht führt nicht nur zum Entfall des Entlassungsschutzes (vgl § 122 [1] Z 4 ArbVG), sondern ist mit durch die Bezirksverwaltungsbehörde zu verhängenden **Verwaltungsstrafe** bis zu 2.180 Euro bedroht (§ 160 [1] ArbVG). Diese Bestimmung kommt allerdings nur zum Tragen, wenn 1. die Tat nach anderen Gesetzen nicht einer strengeren Strafe unterliegt und 2. der Betriebsinhaber binnen sechs Wochen ab Kenntnis von der Übertretung und der Person des Täters, bei der zuständigen Bezirksverwaltungsbehörde einen Strafantrag stellt („Privatanklagedelikt"; § 160 [2] Z 4 ArbVG). Als einschlägige strengere **gerichtliche Strafdrohung** (Freiheitsstrafe bis zu 6 Monaten oder Geldstrafe bis zu 360 Tagessätze) kommt im Kontext des Betriebsrates insbesondere § 122 („Verletzung eines [kraft gesetzlicher Befugnisse zugänglich gewordenen] Geschäfts- oder Betriebsgeheimnisses") StGB in Betracht. Auch dieses Delikt ist als Privatanklagedelikt (zugunsten eines im Interesse an der Geheimhaltung Verletzten) ausgestaltet (§ 122 [5] StGB).

3.2. Soweit Arbeitnehmervertreter vom Betriebsrat in den **Aufsichtsrat** des jeweiligen Unternehmens entsandt werden (§ 110 [1] ArbVG) greifen auch die aktienrechtlichen Verschwiegenheitspflichten für Aufsichtsratsmitglieder (§ 99 iVm § 84 AktG iVm § 110 [3] 5 ArbVG). Die Aufsichtsratsmitglieder der Arbeitnehmerschaft dürfen allerdings den sie entsendenden Betriebsrat soweit informieren, als dies im Interesse der Wahrnehmung der Arbeitnehmerinteressen (§ 38 ArbVG) geboten erscheint.

4. **Hinzu kommen** eine Mehrzahl **gerichtlicher Straftatbestände,** die direkt oder indirekt dem Schutz von Geschäfts- und Betriebsgeheimnissen dienen. Zu verweisen ist hier va auf

   - § 11 („Verletzung von Geschäfts- oder Betriebsgeheimnissen") UWG,

- § 118a („Widerrechtlicher Zugriff auf ein Computersystem") StGB,
- § 119 („Verletzung des Telekommunikationsgeheimnisses"),
- § 119a („Missbräuchliches Abfangen von Daten") StGB,
- § 123 („Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses") oder
- § 63 („Datenverarbeitung in Gewinn- oder Schädigungsabsicht") DSG.

5. Unabhängig von der strafgerichtlichen Verfolgung der Verletzung von Geschäfts- oder Betriebsgeheimnissen (§ 11 UWG) kommt ggf auch eine zivilrechtliche Klage auf **Unterlassung** sowie auf **Schadenersatz** in Betracht (§ 13 UWG; OGH 13. 5. 1992, 9 ObA 93/92).

6.1. Dem Zweck der **EU-weiten Harmonisierung** des Schutzes von Geschäfts- und Betriebsgeheimnissen dient die **Richtlinie (EU) 2016/943** vom 8. 6. 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse). Damit sollen insbesondere die Rechtsschutzmöglichkeiten für Unternehmen, die von einem Bruch der Vertraulichkeit bzw von unrechtmäßiger Nutzung von Geschäfts- und Betriebsgeheimnissen betroffen sind, EU-weit vereinheitlicht werden. Insbesondere sollen solche Geheimnisse auch in Gerichtsverfahren, die zum Zwecke der Rechtsverfolgung angestrebt werden, angemessenen Schutz erfahren.

Als **„Geschäftsgeheimnis"** iSd RL gilt vereinfacht eine Information, die

- geheim,
- aufgrund ihrer Geheimheit von kommerziellem Wert und
- Gegenstand angemessener Geheimhaltungsmaßnahmen ist (Art 2 [1] RL [EU] 2016/943; Bsp: Einkaufs- und Lieferkonditionen, Musterkollektionen; Lieferangebote; Produktionsverfahren; Geschäftsbriefe über die Preisbemessung).
- Als **Inhaber des Geschäftsgeheimnisses** kommen nach der RL sowohl eine juristische als auch eine natürliche Person (Einzelunternehmer) in Betracht (Art 2 [2] RL [EU] 2016/943).

6.2. Die besagte RL war bis 9. 6. 2018 von den Mitgliedstaaten **umzusetzen.** Die österreichische Rechtsordnung soll an die RL im Wege der UWG-Novelle 2018 angepasst werden (vgl §§ 26a bis 26j UWG idF des Entwurfs 58/ME 26. GP 1 ff). Darin finden sich neben einer **Legaldefinition** des Geschäftsgeheimnisses ua ein spezifischer **Unterlassungs-** und **Beseitigungsanspruch,** ein (verschuldensabhängiger) **Schadenersatzanspruch** und spezifische **Sicherungsmittel** sowie Optionen zur **Wahrung** der **Vertraulichkeit** von Geschäftsgeheimnissen **im Verlauf von Gerichtsverfahren.** Letzterer Aspekt soll die bestehende Hemmschwelle zur Einbringung einer „Privatanklage" (§ 11 [3] UWG) senken (Stichwort: Angst vor Geheimnispreisgabe im Zuge des Gerichtsverfahrens).

Die besagte UWG-Novelle 2018 beinhaltet umgekehrt auch **Klarstellungen zum/zur rechtmäßigen Erwerb/Nutzung/Offenlegung** von Geschäftsgeheimnissen. Als praktisch relevante Fälle werden insbesondere die Ausübung der Informations- und Anhörungsrechte durch Arbeitnehmer und Arbeitnehmervertreter, die Informationsweitergabe von Arbeitnehmern an deren Vertreter zwecks legitimer Interessenvertretung oder legitime Überwachungsaktivitäten [Stichwort: Privatdetektiv] genannt (vgl § 26e [2] und [3] UWG idF des Entwurfs 58/ME 26. GP 2 f).

6.3. Aus der **Perspektive** der **Geschäftsführung** kann sich aus der künftig klar umrissenen Definition des Geschäftsgeheimnisses ggf das **Erfordernis** der **Ergänzung** von Geheimhaltungsmaßnahmen (Klauseln in Verträgen mit Geschäftspartnern, Verschwiegenheitsverpflichtung der Mitarbeiter, technische Schutzmaßnahmen) sowie deren entsprechende **Dokumentation** ergeben. Damit sollte verhindert werden, dass die Schutzmechanismen des UWG nicht schon deshalb ins Leere gehen, weil eine Information nicht (mehr) unter den engen Begriff des Geschäftsgeheimnisses fällt.

## ? Frage 7:

Wie ist mit sog **digitalen Partezetteln** zu verfahren, welche auf Websites von Bestattungsunternehmen oder Tageszeitungen gepostet werden? Müssen die älteren Zettel irgendwann gelöscht werden oder können sie unbegrenzte Zeit online bleiben?

**Antwort:**

Die DSGVO gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können allerdings Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen (ErwGr 27). Da auch das DSG keine Regelungen betreffend Verstorbene trifft, fallen die auf Partezetteln enthaltenen **Daten** der **Verstorbenen** nicht unter das Datenschutzrecht. Es gibt insofern auch keine Vorgaben bzw Pflichten zur Löschung.

Anderes gilt aber für auf Partezetteln allenfalls enthaltenen Daten **lebender Verwandter,** anhand derer diese identifiziert werden können. Diese könnten nach einem gewissen Zeit Interesse an einer Entfernung von einer Website haben. Stützt sich die Online-Veröffentlichung auf deren Zustimmung, können sie diese jederzeit widerrufen. Andernfalls könnten sie allenfalls mit dem Wegfall des ursprünglichen Zwecks nach einer gewissen Zeit argumentieren und eine Löschung nach Art 17 (1) lit a) DSGVO verlangen.

# 2. Fragen und Antworten zum räumlichen Anwendungsbereich der DSGVO

## ? Frage 1:

Bedeuten die **strengen Vorgaben** der **DSGVO** für europäische Unternehmen nicht einen gravierenden **Wettbewerbsnachteil gegenüber Unternehmen** aus **anderen Wirtschaftsräumen** (Stichwort: Google, Facebook etc)?

**Antwort:**

**Grundsätzlich Nein.** Zufolge Art 3 (2) DSGVO finden deren Vorgaben nämlich **auch** auf **nicht in der EU niedergelassene Unternehmen** (Verantwortliche oder Auftragsverarbeiter) Anwendung, wenn sie eine Datenverarbeitung durchführen, die im Zusammenhang steht **entweder** mit dem Angebot von Waren oder Dienstleistungen an Personen in der Union, uzw auch „kostenlose" („Facebook"; Suchmaschinen), **oder** mit der Beobachtung des in der Union gezeigten Verhaltens betroffener Personen (Bsp: „Web-Tracking").

## ? Frage 2:

**Binden** spezifische **nationale Arbeitnehmerdatenschutzbestimmungen** bzw lokale Kollektivvereinbarungen (inklusive Betriebsvereinbarungen) **auch ausländische Datenschutz-Aufsichtsbehörden** (als sog „federführende Behörde"; Art 56 [1] DSGVO) oder den Europäischen Datenschutzausschuss, wenn diese die DSGVO-Konformität einer **grenzüberschreitenden Verarbeitung** zu beurteilen haben?

**Antwort:**

**Ja.** Andernfalls würde die Öffnungsklausel des Art 88 (1) DSGVO zugunsten der mitgliedstaatlichen Regelungsbefugnisse auf dem Felde des Beschäftigtendatenschutzes ins Leere laufen. Ein konzernweites Personaldatensystem muss somit nicht nur dem Recht des Mitgliedstaates, in dem sich die Hauptniederlassung eines Konzerns befindet, entsprechen, sondern auch alle allenfalls bestehenden lokalen Anforderungen aus dem Arbeitnehmerdatenschutz erfüllen.

# 3. Fragen und Antworten zum sachlichen Anwendungsbereich der DSGVO

## ? Frage 1:

Ist es nicht problematisch, dass nach der DSGVO **Ungleichheiten** zwischen **privaten** Unternehmen und **öffentlichen** Unternehmen bestehen?

**Antwort:**

Hier handelt es sich um ein **Missverständnis.** Die DSGVO unterscheidet grundsätzlich nicht zwischen dem privaten und dem öffentlichen Sektor bzw zwischen privaten und öffentlichen Verantwortlichen. Die Mitgliedstaaten können allerdings für Datenverarbeitungen für Zwecke der Aufgabenwahrnehmung im öffentlichen Interesse spezifische nationale Regelungen treffen (vgl Art 6 [2] DSGVO). Zudem können die Mitgliedstaaten Behörden und öffentliche Stellen als Verantwortliche von der Sanktionierung in Form von Geldbußen ausnehmen (Art 83 [7] DSGVO). Ob die im DSG vorgesehenen Ausnahmen zugunsten des „öffentlichen Bereichs" nicht zu weit gehen, ist strittig (s insbesondere Pkt 5 der Antwort auf → Frage 5.2, Seite 18).

## ? Frage 2:

Was passiert mit **nichtdigitalen Daten,** die sich im Aktenlager befinden?

**Antwort:**

Die Bestimmungen der DSGVO gelten **nicht nur** für die

- **ganz** oder **teilweise automatisierte Verarbeitung** personenbezogener Daten, **sondern auch für** die
- **nichtautomatisierte Verarbeitung** personenbezogener Daten, **die in einem Dateisystem gespeichert sind oder gespeichert werden sollen** (Art 2 [1] DSGVO).

Dies bedeutet, dass Papierakten bzw sonstige nicht digitale Daten dann unter die DSGVO fallen, wenn sie **nach** zumindest einem **Kriterium durchsuchbar** sind und damit potenziell zur Beschaffung von Informationen über bestimmte oder bestimmbare Personen verwendet werden können. Diesfalls sind insbesondere die Betroffenenrechte (Auskunft etc), aber auch Datensicherheitsmaßnahmen (Zugangskontrolle etc) relevant.

# 4. Fragen und Antworten zum Begriff des „Verantwortlichen“

## ? Frage 1:

Wer ist in der **kommunalen Hoheitsverwaltung** der **„Verantwortliche“** iSd Art 4 (7) DSGVO?

**Antwort:**

1. Zur Bestimmung des Verantwortlichen sind allgemein va folgende Aspekte relevant:
   - Der Verantwortliche muss insbesondere über die Fähigkeit verfügen, die Einhaltung der DSGVO praktisch durchzusetzen (vgl Art 5 [2] [„Prinzip der Verantwortlichkeit“] iVm Art 4 [7] und Art 83 [„Sanktionen“] DSGVO); dies erfordert ein Weisungsrecht oder einen vergleichbaren bestimmenden Einfluss;
   - Es ist stets auf die **konkrete Verarbeitung** personenbezogener Daten zu fokussieren (vgl Art 4 [2] iVm Art 4 [7] DSGVO);
   - Es ist nach dem Verarbeitungs**zweck** zu fragen bzw danach, in wessen Namen bzw Interesse bzw auf wessen Rechnung eine Verarbeitung vorgenommen wird (allfälliger dahinterstehender Rechtsträger!).
   - Schließlich ist für die Identifizierung des Verantwortlichen im Einzelfall auch auf das Organisationsrecht bzw materiengesetzliche **Zuständigkeitszuweisungen** abzustellen (vgl Art 4 [7] 2. HalbS DSGVO, wonach durch Unionsrecht oder mitgliedstaatliches Recht der Verantwortliche beziehungsweise die zu dessen Bestimmung maßgeblichen Kriterien festgelegt werden können).

2.1. Im **eigenen Wirkungsbereich** der Gemeinde (Art 118 [3] B-VG) kommt **bei hoheitlicher Tätigkeit** grundsätzlich ein zweistufiger (innergemeindlicher) Instanzenzug in Betracht, welcher – je nach Bundesland – vom Bürgermeister an den Gemeindevorstand (vgl bspw § 38 [1] Z 2 iVm § 60 [1] Z 1 NÖ GO 1973) oder an den Gemeinderat (vgl bspw § 95 [2] Oö GemO 1990) geht. Daneben kommt ein Instanzenzug gegen erstinstanzliche Bescheide des Gemeindevorstands an den Gemeinderat in Betracht (vgl bspw § 60 [1] Z 2 NÖ GO). Im Falle einer Datenschutzverletzung durch die kommunale Hoheitsverwaltung (bspw Veröffentlichung des Inhalts von Akten oder eines Bescheides im Bauverfahren) kommen insofern je nach Fall va der

   - Bürgermeister,
   - der Gemeindevorstand (Stadtsenat) oder
   - der Gemeinderat und der
   - Magistrat (Statutarstädte, Wien) in Frage.

   **Nicht** als Verantwortliche kommen dagegen weisungsunterworfene Mitarbeiter, Abteilungen oder Geschäftsapparate (außer solche mit gesetzlich angeordneter Behördenfunktion; vgl bspw „Magistrat“ nach § 105 [2] WStV) in Betracht.

2.2. Den **übertragenen Wirkungsbereich** der Gemeinde (Art 119 [1] B-VG) hat der Bürgermeister unter der Weisung des Bundes oder des Landes zu besorgen (Art 119 [2] B-VG). Da die

Entscheidung über die zu verarbeitenden Daten bzw die Zwecke und Mittel hier typischerweise in Bundes- und Landesgesetzen geregelt sind, verbleibt dem Bürgermeister de facto kein Spielraum. Je nach Vollzugsbereich (Bund, Land) sind insofern die obersten weisungsbefugten Organe als Verantwortliche anzusehen (**Bundesminister, Landesregierung;** vgl Art 19 [1] B-VG).

### ? Frage 2:

Wer ist in der **Hoheitsverwaltung** der Länder der **„Verantwortliche“** iSd Art 4 (7) DSGVO?

**Antwort:**

1. Hinsichtlich der der DSGVO zu entnehmenden allgemeinen **Kriterien** zur Bestimmung des Verantwortlichen ist auf Pkt 1 der Antwort auf → Frage 4.1, Seite 9 zu verweisen.
2. Als Verantwortliche kommen demnach va in Betracht:
   - Landesregierung,
   - (ggf) einzelne Mitglieder der Landesregierung,
   - Bezirkshauptmannschaften in Vollziehung von Landesrecht.
3. Zu berücksichtigen ist weiters, dass **durch mitgliedstaatliches Recht** oder **Unionsrecht,** welches Zwecke und Mittel der Verarbeitung vorgibt, auch der Verantwortliche beziehungsweise bestimmte Kriterien seiner Benennung festgelegt werden können (Art 4 [7] 2. HalbS DSGVO; vgl als Bsp „Landesregierung“ als datenschutzrechtlicher Verantwortlicher nach § 35 [3] Oö Stiftungs- und Fondsgesetz). Ein Amt der Landesregierung kommt nur als Verantwortlicher in Betracht, soweit es (punktuell) als Behörde vorgesehen ist.

### ? Frage 3:

Wer ist in der **Hoheitsverwaltung** des Bundes der **„Verantwortliche“** iSd Art 4 (7) DSGVO?

**Antwort:**

1. Hinsichtlich der der DSGVO zu entnehmenden **allgemeinen Kriterien** zur Bestimmung des Verantwortlichen ist auf Pkt 1 der Antwort auf → Frage 4.1, Seite 9 zu verweisen.
2. Demnach kommen in der Hoheitsverwaltung des Bundes in allererster Linie **Behörden** oder Einrichtungen, denen einzelne behördliche Befugnisse übertragen wurden **(Beliehene),** nicht jedoch bspw einzelne mit Approbationsbefugnis ausgestattete weisungsgebundene Organwalter oder Geschäftsapparate (bspw Ministerien) in Betracht. Als Verantwortliche kommen somit insbesondere in Frage:
   - Bundesminister,
   - weisungsfreie Behörden (Bsp: Datenschutzbehörde, öffentliche Universitäten),
   - beliehene Unternehmen (Bsp: Austro Control GmbH, Arbeitsmarktservice),
   - Landespolizeidirektionen,
   - Bezirksverwaltungsbehörden als Sicherheitsbehörden,
   - Bezirkshauptmannschaften (Magistrat) bei mittelbarer Bundesverwaltung,
   - Finanzämter.