Wiederholungsfragen - Datenschutz

1. **Grundlage des österreichischen Datenschutzes:**
   Die Basis ist die EU-Datenschutz-Grundverordnung (DSGVO), die seit dem 25. Mai 2018 unmittelbar gilt – ergänzt durch das nationale Datenschutzgesetz (DSG) in seiner jeweils aktuellen Fassung.

2. **Vollharmonisierung:**
   Vollharmonisierung bedeutet, dass die Datenschutzvorschriften in allen EU-Mitgliedstaaten einheitlich gelten – es herrscht ein gemeinsamer Regelungsrahmen. Nur in ausdrücklich benannten Ausnahmefällen (Öffnungsklauseln) darf von diesem Rahmen abgewichen werden.

3. **Unmittelbare Anwendbarkeit der DSGVO & Öffnungsklauseln:**
   Ja, die DSGVO gilt in Österreich unmittelbar. Öffnungsklauseln erlauben es den Mitgliedstaaten, in bestimmten, gesetzlich benannten Bereichen (z. B. im Beschäftigtendatenschutz) nationale Sonderregelungen zu treffen.

4. **Regelungsinhalt des DSG:**
   Das DSG ergänzt die DSGVO auf nationaler Ebene – es enthält spezifische Bestimmungen, organisatorische Pflichten sowie nationale Bußgeldregelungen und Auslegungsfragen, wo die DSGVO den Staaten Ermessensspielräume lässt.

5. **Betroffene Person:**
   Eine betroffene Person ist jede identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten verarbeitet werden – ausschliesslich natürliche Personen, nicht juristische.

6. **Anwendungsbereich der DSGVO:**

   - **Sachlich:** Sie gilt für alle Vorgänge der Verarbeitung personenbezogener Daten, sei es automatisiert oder als Teil eines Dateisystems.
   - **Räumlich:** Sie erstreckt sich auf Verarbeitungen innerhalb der EU sowie auf Verantwortliche außerhalb, die Waren oder Dienstleistungen an EU-Bürger anbieten oder deren Verhalten beobachten.

7. **Personenbezogene Daten (Beispiele):**
   Informationen, die sich auf eine identifizierte Person beziehen, z. B.:

   - Name und Anschrift
   - E-Mail-Adresse
   - Telefonnummer

8. **Sensible Daten (Beispiele):**
   Daten, die einen besonders schützenswerten Charakter haben, z. B.:

   - Gesundheitsdaten
   - Religiöse Überzeugungen
   - Politische Meinungen

9. **Kombination nicht sensibler Daten zu sensiblen Erkenntnissen:**
   Einzelne, zunächst unscheinbare Angaben (z. B. Vorname, Wohnort und Geburtsdatum) können in

Kombination Rückschlüsse auf sensible Aspekte wie politische oder religiöse Überzeugungen zulassen.

10. **Datenverarbeitung (Formen):**
    Jede operationelle Tätigkeit im Umgang mit personenbezogenen Daten – z. B.:
    - Erhebung (Sammeln)
    - Speicherung (Archivierung)
    - Übermittlung (Weitergabe)

11. **Profiling laut DSGVO:**
    Automatisierte Verarbeitung personenbezogener Daten, um bestimmte persönliche Aspekte (z. B. Vorlieben, Verhalten oder Leistung) zu bewerten oder vorherzusagen.

12. **Rolle des Verantwortlichen:**
    Der Verantwortliche bestimmt Zweck und Mittel der Verarbeitung und trägt die Hauptverantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften.

13. **Rolle des Auftragsverarbeiters:**
    Der Auftragsverarbeiter handelt im Auftrag des Verantwortlichen und verarbeitet Daten gemäß dessen Weisungen – stets unter Einhaltung technischer und organisatorischer Sicherheitsstandards.

14. **Rolle des Empfängers:**
    Ein Empfänger ist jede natürliche oder juristische Person, an die personenbezogene Daten offengelegt werden – er ist jedoch nicht automatisch für die Einhaltung der DSGVO verantwortlich.

15. **Grundsätze der Datenverarbeitung:**
    Damit die Verarbeitung zulässig ist, müssen u. a. folgende Prinzipien beachtet werden:
    - Rechtmäßigkeit, Fairness und Transparenz
    - Zweckbindung
    - Datenminimierung
    - Richtigkeit
    - Speicherbegrenzung
    - Integrität und Vertraulichkeit
    - Rechenschaftspflicht

16. **Datenminimierung vs. Speicherbegrenzung:**
    - **Datenminimierung:** Es werden nur solche Daten erhoben und verarbeitet, die für den jeweiligen Zweck notwendig sind.
    - **Speicherbegrenzung:** Die Daten dürfen nur so lange gespeichert werden, wie es für den Zweck erforderlich ist.

17. **Rechtmäßigkeit der Verarbeitung:**
    Eine Verarbeitung ist rechtmäßig, wenn sie auf einer der in der DSGVO genannten Rechtsgrundlagen beruht (z. B. Einwilligung, Vertragserfüllung, rechtliche Verpflichtung, lebenswichtige Interessen, öffentliche Aufgabe oder berechtigtes Interesse) und alle Grundsätze eingehalten werden.

18. **Verarbeitung sensibler Daten:**
    Sensible Daten dürfen nur verarbeitet werden, wenn eine ausdrückliche Einwilligung vorliegt oder die

Verarbeitung zur Erfüllung gesetzlicher, vertraglicher oder lebenswichtiger Aufgaben notwendig ist – stets unter Beachtung strenger Schutzvorgaben.

19. **Besonderer Schutz strafrechtlich relevanter Daten:**
    Diese Daten unterliegen einer besonders strengen Verarbeitung, meist ausschließlich durch staatliche Stellen oder unter sehr engen gesetzlichen Voraussetzungen, um die Rechte der Betroffenen zu schützen.

20. **Pflichten des Verantwortlichen:**
    Er muss u. a.:

    - Eine rechtmäßige Verarbeitung sicherstellen
    - Transparente Informationspflichten erfüllen
    - Geeignete technische und organisatorische Maßnahmen umsetzen
    - Die Betroffenenrechte gewährleisten
    - Datenschutz-Folgeabschätzungen durchführen, falls erforderlich
    - Datenschutzverletzungen fristgerecht melden

21. **Privacy by Design/Default:**
    Datenschutz muss von Anfang an in Systeme und Prozesse integriert werden (Design) und es dürfen per Voreinstellung nur die zur Erreichung des Zwecks notwendigen Daten verarbeitet werden (Default).

22. **Inhalt des Verarbeitungsverzeichnisses:**
    Der Verantwortliche muss dokumentieren:

    - Zwecke der Verarbeitung
    - Kategorien der betroffenen Personen und Daten
    - Empfänger (einschließlich Drittländern)
    - Geplante Datenübermittlungen
    - Fristen zur Löschung bzw. Speicherbegrenzung
    - Technische und organisatorische Maßnahmen

23. **Meldepflicht bei Datenschutzverletzungen:**
    Wird eine Verletzung festgestellt, die ein Risiko für die Rechte und Freiheiten der Betroffenen darstellt, muss sie innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden – inklusive Art der Verletzung, betroffener Datenmengen, Kontaktdaten des Datenschutzbeauftragten sowie ergriffener Abhilfemaßnahmen.

24. **Ausnahme bei der Meldung an Betroffene:**
    Eine Benachrichtigung an die Betroffenen entfällt, wenn die Verletzung voraussichtlich kein hohes Risiko darstellt oder wenn die Mitteilung einen unverhältnismäßigen Aufwand bedeuten würde – vorausgesetzt, es werden adäquate Maßnahmen zur Risikominderung getroffen.

25. **Datenschutz-Folgeabschätzung (DPIA):**
    Eine systematische Bewertung der Risiken, die mit einer Datenverarbeitung verbunden sind, sowie der Maßnahmen zur Risikominimierung.

26. **Erforderlichkeit einer DPIA:**
    Sie ist verpflichtend, wenn die geplante Verarbeitung voraussichtlich ein hohes Risiko für die Rechte

und Freiheiten natürlicher Personen mit sich bringt – etwa bei großflächiger Überwachung oder bei der Verarbeitung besonderer Kategorien sensibler Daten.

27. **Institutionen, die einen Datenschutzbeauftragten stellen müssen:**
    Öffentliche Stellen sowie private Unternehmen, deren Kerntätigkeit in der regelmäßigen und systematischen Überwachung von Personen oder in der Verarbeitung umfangreicher sensibler Daten besteht.

28. **Voraussetzungen für den Datenschutzbeauftragten:**
    Der DSB muss über fundiertes Fachwissen im Datenschutzrecht verfügen, unabhängig agieren und die nötigen Ressourcen zur Erfüllung seiner Aufgaben erhalten.

29. **Aufgaben des Datenschutzbeauftragten:**

    - Überwachung der Einhaltung der DSGVO und nationaler Vorschriften
    - Beratung des Verantwortlichen und der Mitarbeiter
    - Durchführung von Schulungen und Sensibilisierung
    - Zusammenarbeit mit der Aufsichtsbehörde
    - Anlaufstelle für Betroffene

30. **Zweck von Verhaltensregeln/Code of Conduct:**
    Diese Regeln dienen dazu, branchenspezifische Datenschutzstandards zu formulieren, die Anwendung der DSGVO zu konkretisieren und eine einheitliche Praxis in der Datenverarbeitung zu fördern.

31. **Rechte der betroffenen Personen:**

    - Auskunftsrecht
    - Recht auf Berichtigung
    - Recht auf Löschung („Recht auf Vergessenwerden“)
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit
    - Widerspruchsrecht
    - Rechte im Zusammenhang mit automatisierten Entscheidungen und Profiling

32. **Informationspflichten des Verantwortlichen:**
    Betroffene sind zu informieren über:

    - Identität und Kontaktdaten des Verantwortlichen
    - Zwecke der Verarbeitung
    - Rechtsgrundlage der Verarbeitung
    - Empfänger bzw. Kategorien von Empfängern
    - Speicherdauer oder Kriterien für die Festlegung dieser Dauer
    - Ihre Rechte, inklusive Widerrufs- und Beschwerderecht

33. **Auskunftsrecht der Betroffenen:**
    Es umfasst das Recht, zu erfahren, ob und welche personenbezogenen Daten verarbeitet werden – inklusive Informationen über Verarbeitungszweck, Kategorien der Daten, Empfänger und Speicherdauer.

34. **Recht auf Berichtigung:**
    Die betroffene Person kann die Korrektur unrichtiger oder unvollständiger Daten verlangen.

35. **Gründe für das Recht auf Löschung:**
    Beispielsweise, wenn:
    - Die Daten für den ursprünglichen Zweck nicht mehr benötigt werden
    - Die Einwilligung widerrufen wird
    - Die Verarbeitung unrechtmäßig erfolgt
    - Eine gesetzliche Verpflichtung zur Löschung besteht

36. **Beispiel für Pflicht zur Aufbewahrung:**
    Steuerlich relevante Daten dürfen aufgrund gesetzlicher Aufbewahrungsfristen nicht gelöscht werden, selbst wenn sie ansonsten löschbar wären.

37. **Artikel 20 – Recht auf Datenübertragbarkeit:**
    Betroffene haben das Recht, ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese an einen anderen Verantwortlichen zu übermitteln. Beispiel: Ein Kunde wechselt den Anbieter eines Online-Dienstes und möchte seine gespeicherten Daten übertragen.

38. **Hauptanwendungsfall des Widerspruchsrechts:**
    Vor allem bei der Verarbeitung auf Basis berechtigter Interessen oder im Rahmen von Direktwerbung – hier kann die betroffene Person jederzeit Widerspruch einlegen.

39. **Triftige Gründe zur Einschränkung betroffener Rechte:**
    Einschränkungen können zulässig sein, wenn überwiegende schutzwürdige Interessen (z. B. öffentliche Sicherheit, die Rechte Dritter oder gesetzliche Pflichten) entgegenstehen – vorausgesetzt, diese Interessen überwiegen die Rechte der betroffenen Person.

40. **Überwachung der DSGVO-Anwendung:**
    In jedem EU-Mitgliedstaat überwacht eine nationale Aufsichtsbehörde (in Österreich die Datenschutzbehörde) die Einhaltung der DSGVO.

41. **Untersuchungsbefugnisse der Behörde:**
    Die Behörde kann Vor-Ort-Kontrollen durchführen, Unterlagen anfordern, Mitarbeiter befragen, Untersuchungen leiten und bei Verstößen Sanktionen (z. B. Bußgelder) verhängen.

42. **Kooperationsverfahren mit der EU-Kommission:**
    Das sogenannte „One-Stop-Shop"-Verfahren ermöglicht eine koordinierte Zusammenarbeit der nationalen Aufsichtsbehörden bei grenzüberschreitenden Verarbeitungen.

43. **Beschwerde bei Datenschutzverletzungen:**
    Betroffene können sich an die zuständige nationale Aufsichtsbehörde wenden – in Österreich an die Datenschutzbehörde.

44. **Anspruch der Betroffenen gegenüber dem DSGVO-Verletzer:**
    Betroffene haben Anspruch auf Schadensersatz für materielle und immaterielle Schäden – die Entscheidung darüber trifft letztlich ein Gericht.

45. **Höhe der Geldbußen:**
    Geldbußen können bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes betragen – je nachdem, welcher Wert höher ist.

46. **Drei konkrete Tatbestände:**
    - Unrechtmäßige bzw. intransparente Verarbeitung personenbezogener Daten
    - Versäumnis, den Informationspflichten nachzukommen
    - Fehlende oder unzureichende technische/organisatorische Sicherheitsmaßnahmen

47. **Österreichs zusätzliche Sanktionen (Artikel 83):**
    Neben den EU-weiten Bußgeldern sieht das österreichische Recht ergänzende Sanktionen und konkrete, teilweise verschärfte Bußgeldvorgaben vor, um Datenschutzverstöße gezielt zu ahnden.

48. **Institutionen des Datenschutzes in Österreich:**
    - Datenschutzbehörde
    - Datenschutzrat
    - Datenschutzbeauftragte in öffentlichen Einrichtungen und Unternehmen

49. **Aufgaben des Datenschutzrats:**
    Er berät die Regierung und die Datenschutzbehörde, unterstützt bei der Auslegung und Weiterentwicklung des Datenschutzrechts und fördert den Austausch zwischen den Akteuren.

50. **Aufgaben der Datenschutzbehörde:**
    Sie überwacht und setzt die Datenschutzvorschriften durch, bearbeitet Beschwerden, führt Prüfungen durch und verhängt Sanktionen bei Verstößen.

51. **Bestellungsdauer des Leiters der Datenschutzbehörde:**
    Der Leiter wird üblicherweise für eine Amtszeit von etwa 5 Jahren bestellt – die Ernennung erfolgt durch den zuständigen Bundesminister (in der Regel des Innern).