Datenschutz-Grundverordnung Erkenntnisse

Fortbildung für die Leiter des Verwaltungsdienstes im Bezirks- bzw Abschnittsfeuerwehrkommando, Tulln 24.11.2018

Mag. Harald Strahberger, Rechtsanwalt

Inhalt

- Neuerungen aufgrund der DSGVO
- Themen für die Praxis
  - Personenbezogene Daten
  - Verarbeitung
  - Rechtmäßigkeit der Datenverarbeitung
  - Informationspflichten nach der DSGVO
  - Auskunftserteilung
  - Data-Breach
  - Judikatur
- Fragen

Grundzüge der DSGVO und des DSG 2018 (I)

- Keine Meldepflicht mehr bei der Datenschutzbehörde
  - Abschaffung des Datenverarbeitungsregisters
- Stärkere Verantwortung für Verantwortliche und Auftragsverarbeiter
  - Verantwortlicher: natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet („Herr über die Daten“)
  - Auftragsverarbeiter: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet
- privacy by design und privacy by default
  - geeignete technische und organisatorische Maßnahmen zu treffen, damit die Verarbeitung personenbezogener Daten den Anforderungen der DSGVO genügt und die Rechte der betroffenen Personen geschützt werden
  - datenschutzrechtliche Voreinstellungen sollen sicherstellen, dass grds nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden

Grundzüge der DSGVO und des DSG 2018 (II)

- Verzeichnis von Verarbeitungstätigkeiten
  - ersetzt die Meldung im Datenverarbeitungsregister bei der Datenschutzbehörde
  - folgende Angaben:
    - Name und die Kontaktdaten des für die Verarbeitung Verantwortlichen;
    - Zwecke der Verarbeitung
    - Beschreibung der Kategorien von betroffenen Personen und der Kategorien personenbezogener Daten
    - die Kategorien von Datenempfängern
    - Übermittlungen von Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation
    - die Fristen für die Löschung der verschiedenen Datenkategorien
    - allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
  - Pflicht besteht nicht:
    - bei weniger als 250 Mitarbeiter, sofern
    - die Verarbeitung Kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt
    - Verarbeitung nur gelegentlich erfolgt
    - keine besonderen Datenkategorien bzw strafrechtlich relevante Daten verarbeitet werden

Grundzüge der DSGVO und des DSG 2018 (III)

- Verpflichtung zur Meldung von Data-Breaches
  - Meldung an die nationalen Datenschutzbehörden
  - Meldung an die betroffenen Personen
- Pflicht zur Durchführung einer Datenschutzfolgenabschätzung bei Verarbeitungsvorgängen, die aufgrund der Art, des Umfangs, der Umstände und der Zweck vorrausichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben
  - Konsultation der Aufsichtsbehörde, wenn aus der der Datenschutzfolgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der für die Verarbeitung Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft
- Pflicht zur Bestellung eines Datenschutzbeauftragten (öffentliche Stellen verpflichtend)

Grundzüge der DSGVO und des DSG 2018 (IV)

- Informationspflichten und Betroffenenrechte
  - Auskunftsrechte (zB welche Daten werden verarbeitet und warum?)
  - Recht auf Berichtigung
  - Recht auf Löschung und „Vergessenwerden“
  - Recht auf Einschränkung der Verarbeitung
  - Mitteilungspflicht bei Berücksichtigung, Löschung oder Einschränkung an alle Empfänger
  - Recht auf Datenübertragbarkeit
  - Widerspruchsrecht
  - Regelung betreffend automatisierte Generierung von Einzelentscheidungen einschließlich profiling
- Erweiterung der Befugnisse und Aufgaben der Aufsichtsbehörden

Grundzüge der DSGVO und des DSG 2018 (V)

- Hohe Geldstrafen (Art 83 DSGVO)
  - Verstöße gegen allgemeine Compliance-Pflichten: Strafen bis zu Euro 10 Mio oder 2% des weltweiten Jahresumsatzes
  - Verstöße gegen Betroffenenrechte: Strafen bis zu Euro 20 Mio oder 4% des weltweiten Jahresumsatzes
  - gemäß § 30 Abs 5 DSG 2018 können keine Geldstrafen gegen Behörden, öffentliche Stellen und gegen Körperschaften des öffentlichen Rechts verhängt werden.
  - ABER ACHTUNG: keine Befreiung von Schadenersatzforderungen aufgrund zivilrechtlicher Schadenersatzklagen, zB unzulässige Bildverwendung!

Praxisthemen – Personenbezogene Daten (I)

- Personenbezogene Daten (Art 4 Z 1 DSGVO):
  - alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen;
  - identifizierbar = Person direkt oder indirekt, insb mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann
- Typische Beispiele:
  - Name, Geburtsdatum,
  - Kontaktdaten zB Adresse, E-Mail Adresse, Telefonnummer
  - Sozialversicherungsnummer
  - Fotos, Videoaufnahmen

Praxisthemen – Personenbezogene Daten (II)

- Besondere Kategorien personenbezogener Daten (Art 9 DSGVO):
  - Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen
  - genetische und biometrische Daten,
  - Gesundheitsdaten
  - Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person
- Beispiele:
  - Religion bzw Religionsbekenntnis
  - Erfassung des Herkunftslandes
  - Gesichtsbilder (Passbilder), Fingerabdrücke
  - Blutgruppe
  - Krankengeschichte des Betroffenen, zB Operationen, Behinderungen, Krankheitsrisiken
  - Familienstand

Praxisthemen – Personenbezogene Daten (III)

- Pseudonymisierte personenbezogene Daten sind identifizierbar!
  - Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden
- Anonyme Informationen unterliegen nicht dem Datenschutz
  - Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.
- Beispiele
  - Pseudonymisierung = anstatt der Datensätze der Mitglieder werden individuelle Nummern verwendet aufgrund die Datensäte wieder aufgerufen werden können
  - Anonymisierung = Datensätze der Mitglieder werden gänzlich gelöscht und durch Platzhalter ersetzt

Praxisthemen – Verarbeitung

- Verarbeitung personenbezogener Daten (Art 4 Z 2 DSGVO)
  - mit oder ohne Hilfe automatisierter Verfahren
  - Erheben, Erfassen, Organisieren, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder die Verknüpfung, Einschränkung, Löschen oder die Vernichtung
  - Entscheidend, dass Daten in einem Dateisystem gespeichert sind
    - jede strukturierte Sammlung personenbezogener Daten
    - nach bestimmten Kriterien zugänglich sind
    - dezentral oder nach funktionalen oder geographischen Gesichtspunkten geordnet
    - dh nicht nur elektronische Dateisysteme, sondern auch Karteikarten oder entsprechend strukturierte Papierakten usw
- Beispiele
  - Erfassen von Bewerbern, Spendern, Geschädigten
  - Dienstaufzeichnungen
  - Einsatzfotos oder Fotos von Veranstaltungen auf einer Webseite oder auf Social Media Plattformen

Praxisthemen – Rechtmäßigkeit (I)

- Allgemeine Grundsätze der Datenverarbeitung:
  - Rechtmäßigkeit
    - auch nach der DSGVO gilt, dass grds jede Datenverarbeitung verboten ist, außer sie ist erlaubt
    - Datenverarbeitung nur aufgrund einer entsprechenden Rechtsgrundlage (Art 6 und Art 9 DSGVO)
  - Verarbeitung nach Treu und Glauben
    - keine Datensammlung nach dem Motto „weil ich es kann“
  - Transparenz
    - Information des Betroffenen zur Verarbeitung der Daten leicht zugänglich, verständlich und in klarer und einfacher Sprache
    - eingeführt werden standardisierte Bildsymbole zur einfachen Information
- Grundsatz der Zweckbindung:
  - legitimer Zweck bereits bei der Erhebung eindeutig festzulegen, zB im Verarbeitungsverzeichnis
  - keine Weiterverarbeitung, wenn mit dem ursp Zweck nicht vereinbar

Praxisthemen – Rechtmäßigkeit (II)

- Grundsatz der Datenminimierung
  - Verarbeitung soll dem Zweck angemessen und auf das notwendige Maß beschränkt werden
- Grundsatz der Richtigkeit
- Grundsatz der Speicherbegrenzung
  - Speicherung nur solange, wie es für die Zwecke, für die sie vereinbart werden, erforderlich ist
- Datenintegrität und Vertraulichkeit
  - setzen geeigneter technischer und organisatorischer Maßnahmen
  - Schutz vor unbefugter oder unrechtmäßiger Verarbeitung sowie unbeabsichtigtem Datenverlust,- zerstörung oder –schädigung

Praxisthemen – Rechtmäßigkeit (III)

- Rechtsgrundlagen (Art 6 DSGVO)
  - Einwilligung
  - Vorliegen eines Vertrages oder der Erforderlichkeit der Durchführung vorvertraglicher Maßnahmen
  - Vorliegen einer rechtlichen Verpflichtung des Verantwortlichen
    - zB Erfassen und Bekanntgabe von Spendern aufgrund des EStG iVm der BAO
  - Vorliegen lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person
  - Erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde
  - Erforderlich zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten,
    - sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen,
    - insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Praxisthemen – Rechtmäßigkeit (IV)

- Einwilligung der betroffenen Person (Art 4 Z 11 DSGVO)
  - jede freiwillige
    - ACHTUNG: Koppelungsverbot (Art 7 Abs 4 DSGVO) - zB wenn die Aufnahme eines Bewerbers von der Einwilligung zu einer Verarbeitung seiner personenbezogenen Daten abhängt
  - für den bestimmten Fall
    - Wenn in einer Erklärung mehrere Einwilligungen erteilt werden sollen, dann hat dies in verständlicher und leicht zugänglicher Form sowie in einfacher Sprache zu erfolgen (Art 7 Abs 2 DSGVO)
  - in informierter Weise
    - Zweck der vorgenommenen Verarbeitungsvorgänge
  - unmissverständlich abgegebene Willenserklärung
  - in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung
    - Anklicken bzw Anhaken eines Kästchens
    - Nicht stillschweigende Einwilligung ohne Zutun der betroffenen Person
- Nachweispflicht des Verantwortlichen (Art 7 Abs 1 DSGVO)
- Recht des Betroffenen seine Einwilligung jederzeit zu widerrufen (Art 7 Abs 3 DSGVO)

Praxisthemen – Rechtmäßigkeit (V)

- Rechtsgrundlagen besondere Kategorien personenbezogener Daten (Art 9 DSGVO)
  - Einwilligung
  - Ausübung von Rechten aus dem Arbeitsrecht der sozialen Sicherheit und des Sozialschutzes
  - Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person
  - Datenverarbeitung durch einen sog Tendenzbetrieb
  - die betroffene Person hat die Daten offensichtlich öffentlich gemacht
  - Zur Geltendmachung von Rechtsansprüchen
  - Erforderlich aufgrund eines erheblichen öffentlichen Interesses, wobei die Verarbeitung auf gesetzlicher Grundlage basiert
  - Gesundheitsvorsorge, Arbeitsmedizin, medizinische Diagnostik
  - Aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
  - Erforderlichkeit für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke sowie für statistische Zwecke

Praxisthemen – Informationspflichten (I)

- Informationspflicht, wenn Daten vom Betroffenen selbst stammen (Art 13 DSGVO)
  - Namen und Kontaktdaten des Verantwortlichen
  - ggf Kontaktdaten des Datenschutzbeauftragten
  - Verarbeitungszwecke und Rechtsgrundlagen der Verarbeitung
  - im Falle der Verarbeitung aufgrund berechtigter Interessen, die berechtigten Interessen, die verfolgt werden
    - Nicht möglich bei besonderen Kategorien von personenbezogenen Daten
  - die Empfängerkategorien
  - Information über die Übermittlung der Daten in ein Drittland oder an eine internationale Organisation
    - Information über das Vorhandensein bzw das Fehlen eines Angemessenheitsbeschlusses der Europäischen Kommission
    - Einhaltung entsprechender datenschutzrechtlicher Garantien bei der Übermittlung
  - Dauer der Datenspeicherung bzw die Kriterien für die Festlegung der Dauer
  - Betroffenenrechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch
  - Möglichkeit des Widerrufs einer Einwilligung

Praxisthemen – Informationspflichten (II)

- Informationspflicht, wenn Daten vom Betroffenen selbst stammen (Art 13 DSGVO) - Fortsetzung
  - Beschwerdemöglichkeit bei der Aufsichtsbehörde
  - ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte
  - ggf das Bestehen automatisierter Entscheidungsfindung inkl aussagekräftiger Informationen über die involvierte Logik und die Tragweite der Entscheidung
  - Sollen die Daten für einen anderen als den urspr Zweck weiterverarbeitet werden, auch die Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen hierzu
- Die Information ist zum Zeitpunkt der Erhebung zur Verfügung zu stellen!
- Keine Informationspflicht, wenn der Betroffene die Informationen bereits erhalten hat oder generell darüber verfügt

Praxisthemen – Informationspflichten (III)

- Informationspflicht, wenn Daten nicht beim Betroffenen erhoben werden (Art 14 DSGVO)
  - Namen und Kontaktdaten des Verantwortlichen
  - ggf Kontaktdaten des Datenschutzbeauftragten
  - Verarbeitungszwecke und Rechtsgrundlagen der Verarbeitung
  - **Kategorien der verarbeiteten Daten**
  - die Empfängerkategorien
  - Information über die Übermittlung der Daten in ein Drittland oder an eine internationale Organisation
    - Information über das Vorhandensein bzw das Fehlen eines Angemessenheitsbeschlusses der Europäischen Kommission
    - Einhaltung entsprechender datenschutzrechtlicher Garantien bei der Übermittlung
  - Dauer der Datenspeicherung bzw die Kriterien für die Festlegung der Dauer
  - berechtigte Interessen
  - Betroffenenrechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch
  - Möglichkeit des Widerrufs einer Einwilligung

Praxisthemen – Informationspflichten (IV)

- Informationspflicht, wenn Daten nicht beim Betroffenen erhoben werden (Art 14 DSGVO) - Fortsetzung
  - Beschwerdemöglichkeit bei der Aufsichtsbehörde
  - Quelle der Daten und ob sie ggf aus öffentlich zugänglichen Quellen stammen
  - ggf das Bestehen automatisierter Entscheidungsfindung inkl aussagekräftiger Informationen über die involvierte Logik und die Tragweite der Entscheidung
  - Informationen über Zweckäderungen
- Zeitpunkt Information
  - nur interne Verarbeitung – längstens jedoch innerhalb eines Monats
  - Daten zur Kommunikation mit dem Betroffenen verwendet – spätestens zum Zpkt der ersten Mitteilung an diesen
  - Offenlegung an einen anderen Empfänger beabsichtigt – spätestens zum Zpkt der Offenlegung

Praxisthemen – Informationspflichten (V)

- Keine Informationspflicht gemäß Art 14 DSGVO, wenn
  - der Betroffene die Informationen bereits erhalten hat oder generell darüber verfügt
  - Erteilung sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde
  - dies durch Rechtsvorschriften der Union oder der Mitgliedstaaten ausdrücklich geregelt ist
  - die Daten dem Berufsgeheimnis oder einer satzungsmäßigen Geheimhaltungspflicht unterliegen und daher vertraulich behandelt werden müssen

Praxisthemen – Auskunftsrecht (I)

- Auskunftsrecht der betroffenen Person (Art 15 DSGVO)
  - Bestätigung darüber, ob bestimmte personenbezogene Daten verarbeitet werden
    - Genügt, dass zB Daten gespeichert werden
  - Verarbeitungszwecke
  - Kategorien personenbezogener Daten
  - Empfänger oder Kategorien von Empfängern
  - geplante Dauer der Speicherung
  - alle verfügbaren Informationen über die Herkunft der Daten, wenn diese nicht bei der betroffenen Person erhoben wurden
  - im Falle von Profiling – Angaben zur verwendeten Logik sowie den Auswirkungen der einer derartigen Verarbeitung
  - Aufklärung über das Recht auf
    - Berichtigung
    - Löschung
    - Einschränkung
    - Widerspruch gegen die Verarbeitung
    - Beschwerde bei der Aufsichtsbehörde

Praxisthemen – Auskunftsrecht (II)

- Mitwirkungspflicht der betroffenen Partei in ErwG 63 DSGVO nur angedeutet
- Recht auf eine unentgeltliche Kopie
- Auskunftsbegehren ist grds unverzüglich, spätestens binnen eines Monats nach Einlangen zu erteilen (Art 12 Abs 3 DSGVO)
  - Bei komplexen Begehren kann die Frist auf zwei Monate verlängert werden

Praxisthemen – Auskunftsrecht (Checkliste)

- Prozess, wie das Recht auf Auskunft gewährt wird?
- Sind die Daten, die beauskunftet bzw die Informationen, die erteilt werden müssen, auffindbar - wo?
- Im Fall der Verweigerung der Auskunft – Verständigung der betroffenen Person innerhalb der Frist von einem Monat
- Vertretbare Mittel benutzen, um die Identität der betroffenen Person zu überprüfen
- Betroffene Person zur Mitwirkung auffordern, insb bei umfangreichen Auskunftsersuchen
- Sicherstellung, dass die Auskunftserteilung unverzüglich bzw spätestens innerhalb eines Monats erfolgt bzw erfolgen kann
- Sicherstellung, dass auch bei einer Einschränkung der Verarbeitung die gesperrten Daten beauskunftet werden?
- Rechtzeitige Information der betroffenen Person bei voraussichtlicher Überschreitung der Monatsfrist für die Erteilung der Auskunft
- Sicherstellung, dass eine Übermittlung der Auskunft sowohl in schriftlicher als auch in elektronischer Form erfolgen kann
- Auskunftserteilung in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache
- Prüfung bei der Auskunftserteilung, dass bei der Zurverfügungstellung einer Kopie der personenbezogenen Daten an die betroffene Person die Rechte und Freiheiten anderer betroffener Personen nicht beeinträchtigt werden
- Dokumentation der Tatsache einer Auskunftserteilung

Praxisthemen – Data Breach (I)

- Data Breach: Möglichkeit natürliche Person einen physischen, materiellen oder immateriellen Schaden erleiden könnte, wie etwa den Verlust der Kontrolle über ihre personenbezogenen Daten oder eine Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder – betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung usw (ErwG 85 DSGVO)
- Beispiele:
  - Verlust von Datenträgern, zB USB-Stick, Handys, Laptops
  - Datenlecks
  - Hacking
  - Fehlen von technischen organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten, zB schlecht gesicherte Serverräume, keine Passwörter

Praxisthemen – Data Breach (II)

- Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art 33 DSGVO)
  - unverzüglich, möglichst binnen 72 Stunden
  - nachdem ihm die Verletzung bekannt wurde
  - an die zuständige Aufsichtsbehörde
- Meldung hat zumindest folgende Informationen zu umfassen:
  - Beschreibung der Art der Verletzung
    - soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
  - Namen und die Kontaktdaten des Datenschutzbeauftragten bzw einer sonstigen Anlaufstelle für weitere Informationen
  - Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
  - Eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und ggf Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Praxisthemen – Data Breach (III)

- Dokumentationspflicht des Verantwortlichen in Bezug auf die Verletzung einschließlich aller iZm der Verletzung stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen
  - muss der Aufsichtsbehörde die Überprüfung ermöglichen
- eine Meldung an die Aufsichtsbehörde kann unterbleiben, wenn die Verletzung nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (siehe ErwG 85)
- Meldung an die betroffene Person (Art 34 DSGVO)
  - wenn voraussichtlich ein hohes Risiko für die persönlichen Rechte und die Freiheiten der natürlichen Person
  - grds die gleichen Informationen wie an die Aufsichtsbehörde
  - keine Meldung an die betroffene Person wenn:
    - geeignete technische und organisatorische Maßnahmen angewendet werden (Verschlüsselung)
    - Schutzmaßnahmen implementiert sind, aufgrund derer Verletzungen im Nachhinein unterbunden werden können
    - unverhältnismäßigen Aufwand darstellen würde

Praxisthemen – Data Breach (Checkliste)

- Prozess, wie im Falle einer Datenschutzverletzung vorzugehen ist?
- Krisenstab zur Bewältigung von Datenschutzverletzungen einrichten (im Vorhinein) – erforderlichenfalls erweitern, zB Datenschutzexperten, Forensiker udgl
- Festlegung klarer und verständlicher Regeln für die Handhabung der Datenschutzverletzung (Meldeweg – Letztverantwortung)
- Zuordnung der Aufgaben im Krisenstab
  - Analyse und Bewertung der Datenschutzverletzung
  - Risikoanalyse
  - Entscheidung über die Meldung/Nichtmeldung
  - Entscheidung über die Art der Information
  - Maßnahmen zur Milderung der Folgen der Datenschutzverletzung
- Entwurf einer Mustervorlage für den Analysebericht mit zumindest folgendem Inhalt:
  - Datum und Uhrzeit des Vorfalls
  - Art und Ursachen der Datenschutzverletzung
  - Betroffene IT-Systeme
  - Anzahl der betroffenen Personen
  - Betroffene personenbezogene Daten
  - Getroffene Schutzmaßnahmen, um die Auswirkungen der Datenschutzverletzung zu mildern
  - Technische und organisatorische Maßnahmen, um eine Datenschutzverletzung in Zukunft zu verhindern
- Entwurf eines Musters für die Benachrichtigung an die betroffene Person mit zumindest folgendem Inhalt:
  - Art der Datenschutzverletzung
  - Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Auskunftsstelle
  - Beschreibung der wahrscheinlichen Folgen der Verletzung
  - Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und ggf Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- Sicherstellung, dass es zur Umsetzung von entsprechenden Verbesserungsmaßnahmen kommt
- Ggf sollte ein Probelauf über eine Datenschutzverletzung durchgeführt werden

Praxisthemen – Judikatur (I)

- **DSB-D123.070/0005-DSB/2018 vom 13.09.2018**: eine betroffene Person hat kein Recht, eine Pseudonymisierung zu fordern; aus der DSGVO kein Recht abzuleiten, wonach eine betroffene Person spezifische Datensicherheitsmaßnahmen iSv Art 32 DSGVO von einem Verantwortlichen verlangen könnte; ebenso wenig kann eine betroffene Person spezifische Maßnahmen zur Datenminimierung iSv Art 5 DSGVO verlangen
- **DSB-D123.085/0003-DSB/2018 vom 27.8.2018**: Bewerberdaten dürfen für den Zweck der Abwehr von etwaigen Rechtsansprüchen wegen Diskriminierung bei Begründung eines Arbeitsverhältnisses für einen Zeitraum von 6 Monaten sowie einen angemessenen Zeitraum eines Nachlaufes (1 Monat) aufbewahrt werden; zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dürfen Daten aufbewahrt (gespeichert) werden, wenn der Rechtsgrund des Anspruches konkret benannt wird, und auch die Frist klar und deutlich festgelegt ist; der Verantwortliche muss darlegen können, welche konkreten zukünftigen Verfahren auf welcher Grundlage anhängig gemacht werden könnten und inwiefern durch derartige Verfahren eine Notwendigkeit zur weiteren Aufbewahrung der personenbezogenen Daten begründet wird.
- Widerspruch zu **DSB-D216.471/0001-DSB/2018 vom 28.5.2018**, wonach Verjährungsfristen keine Rechtfertigung für eine Speicherung bis zu deren Ablauf darstellen – 10-Jährige Frist nach BAO daher kein geeigneter Rechtfertigungsgrund für Speicherung

Praxisthemen – Judikatur (II)

- Geldstrafe iHv EUR 4.800,-, weil eine Videoüberwachung nicht ausreichend gekennzeichnet war und ein großer Teil des Gehsteigs von der Anlage mitaufgezeichnet wurde
- Der baden-württembergische Datenschutzbeauftragte teilte am 15.11.2018 mit, dass gegen den Betreiber von Knuddels.de eine Geldbuße von EUR 20.000,- verhängt worden sei, da die Passwörter von Nutzern unverschlüsselt gespeichert worden seien. Damit hätte das Unternehmen keine ausreichenden technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten gesetzt
- EUR 400.000,- Strafe für ein Krankenhaus in Portugal, weil zu viele Personen Zugriff auf Patientendaten gehabt hätten; IT-Techniker Zugang zu Daten verschafft, die eigentlich nur von Ärzten hätten eingesehen werden dürfen und durch einen Test sei festgestellt worden, dass solch ein Profil mit unbegrenztem Zugang problemlos erstellt werden konnte. Hinzukam, dass obwohl 2018 nur 296 Ärzte in dem Krankenhaus arbeiten, in dem System insgesamt 985 aktive Benutzer als „Arzt“ registriert waren

Kontakt

Mag. Harald Strahberger
Rechtsanwalt

Kontakt:
+43 678 1277 255
harald.strahberger@gmail.com

Beruflicher Werdegang
Universität Wien (2009 Mag. iur.), 2010 Gerichtspraxis, 2010-2015 Rechtsanwaltsanwärter bei bpv Hügel Rechtsanwälte OG, 2015-2016 Rechtsanwalt bei bpv Hügel Rechtsanwälte OG, 2016-2017 Rechtsanwalt bei EY Law – Pelzmann Gall Rechtsanwälte GmbH, seit 2017 Rechtsanwalt bei bpv Hügel Rechtsanwälte GmbH

Seit 2018 zertifizierter betrieblicher Datenschutzbeauftragter

Beratungsschwerpunkte
Öffentliches Wirtschaftsrecht, Vergaberecht, Umweltrecht