Your World First

CMS Law.Tax

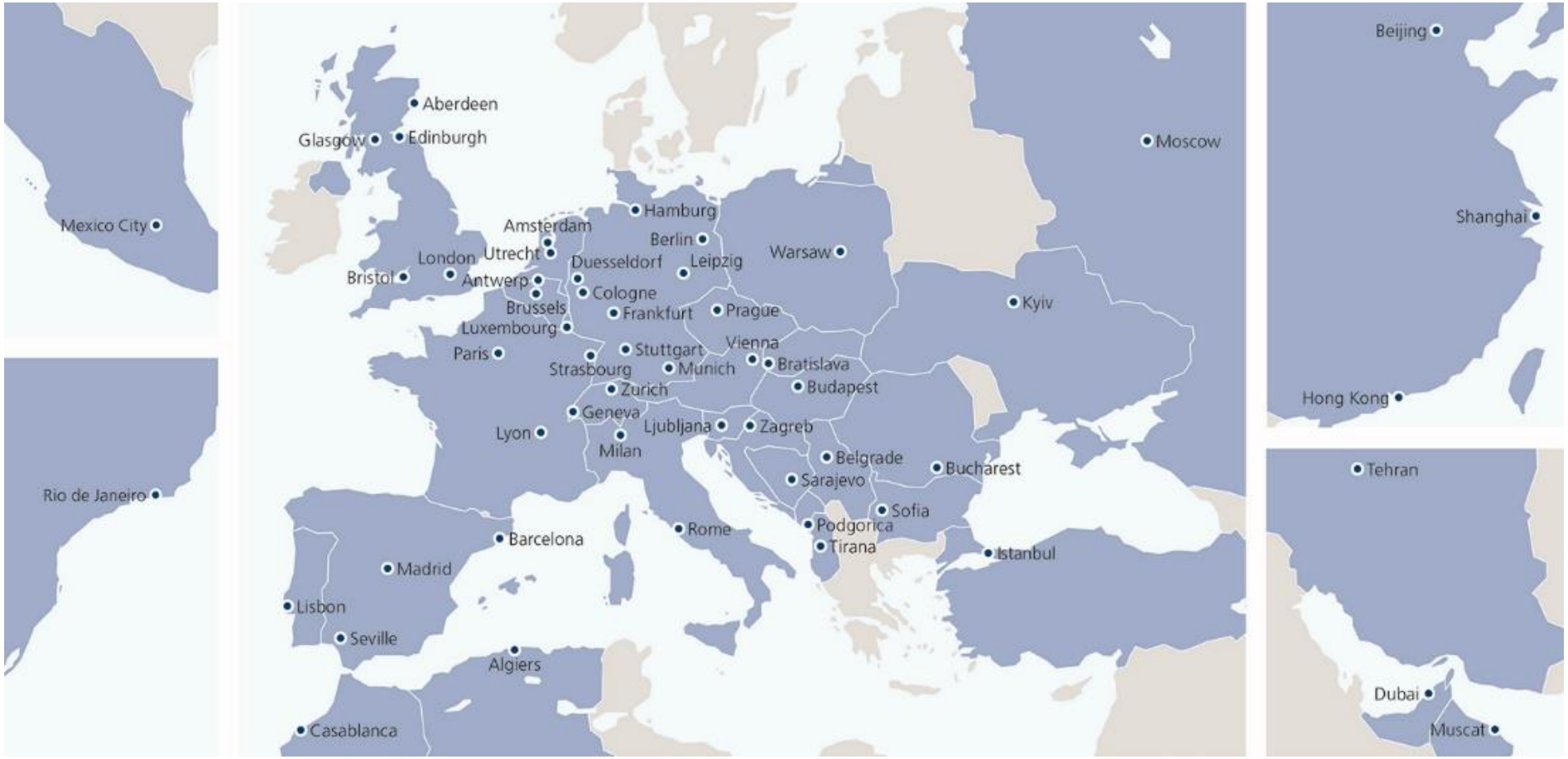
EU Datenschutz-Grundverordnung (DSGVO)

Trends und erste Erfahrungen nach Inkrafttreten

Dr. Johannes Juranek, Partner, CMS Austria & CEE
JUDr. Jozef Čupa, LL.M., Senior Associate, CMS Slovakia
Mgr. Kristína Szajkóová, Staatsrätin, Datenschutzamt der Slowakischen Republik

Über CMS

CMS Rechtsanwaltskanzleien



Die EU Datenschutz-Grundverordnung

Überblick über die heutigen Themen

- DSGVO Begriffe
- Rechtmäßigkeit der Verarbeitung (Art 6 und 9)
- Rechte der Betroffenen
- Umgang mit Auskunfts- und Löschersuchen
- Neuigkeiten und häufige Fragen
- Aufbewahrungsgrundsätze und -fristen
- Data Breach

Ein paar Begriffe…

Personenbezogene Daten

„alle **Informationen**, die sich auf eine **identifizierte** oder **identifizierbare natürliche** Person (‚**betroffene Person**‘) beziehen“

Besondere Kategorien personenbezogener Daten („sensible Daten“)

„personenbezogene Daten, über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit, das Sexualleben oder die sexuelle Orientierung, sowie **genetische oder biometrische Daten**“

Verarbeitung

„**jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe** im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“

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**“

Auftragsverarbeiter

„**natürliche oder juristische Person,** Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten **im Auftrag des Verantwortlichen** verarbeitet“

Rechtmäßigkeit der Verarbeitung (Art 6)

Rechtmäßigkeit der Verarbeitung besonderer Kategorien von personenbezogenen Daten (Art 9)

Rechte des Betroffenen (Art 15 – 21)

- Auskunftsrecht (Art 15)
- Recht auf Berichtigung (Art 16)
- Recht auf Löschung („Recht auf Vergessenwerden“, Art 17)
- Recht auf Einschränkung der Verarbeitung (Art 18)
- Recht auf Datenübertragberkeit (Art 20)
- Widerspruchsrecht (Art 21)
- Beschwerderecht bei einer Aufsichtsbehörde (Art 13(2)(d))

Recht auf Löschung („Recht auf Vergessenwerden“, Art 17)

- Keine Regelung der Beweislast
- Identitätsnachweis nur im Zweifelsfall
  - z.B. Telefonanruf, Phantasie-E-Mail-Adresse
- Frist
  - sofort, spätestens jedoch 1 Monat nach Eingang des Löschbegehrens
  - kann auf weitere 2 Monate verlängert werden
- **Verweigerung der Löschung (Art 17(3))**
  - Erfüllung einer **rechtlichen Verpflichtung;**
  - zu Archivierungszwecken im öffentlichen Interesse, zu wissenschaftlichen oder historischen Forschungszwecken oder **zu statistischen Zwecken**;
  - Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen**;
  - Offenkundig unbegründete Anfrage oder **Exzessivität** (insbesondere im Fall von häufiger Wiederholung; Art 12(5))

Recht auf Löschung („Recht auf Vergessenwerden“, Art 17)

– Begründete Anfrage
  - Personenbezogene Daten sind für die Zwecke, für die sie erhoben oder anderweitig verarbeitet wurden, nicht mehr erforderlich
  - der Betroffene widerruft die Einwilligung (und es gibt keinen anderen Rechtsgrund für die Verarbeitung)
  - der Betroffene widerspricht der Verarbeitung, die aufgrund berechtigter Interessen oder Direktmarketing (einschließlich Profiling) erfolgt
  - unzulässige Verarbeitung
  - die Löschung ist aufgrund einer rechtlichen Verpflichtung in den Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, erforderlich
  - personenbezogene Daten wurden im Zusammenhang mit dem Angebot von Diensten der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben

Recht auf Löschung („Recht auf Vergessenwerden“, Art 17)

- **Mitteilungspflicht des Verantwortlichen**
  - Der Verantwortliche informiert jeden Empfänger, dem die personenbezogenen Daten gegenüber offengelegt wurden, über die Löschung
    - es sei denn, dies ist unmöglich oder mit unverhältnismäßigem Aufwand verbunden
  - Der Verantwortliche informiert den Betroffenen über diese Empfänger, wenn der Betroffene dies verlangt

Recht auf Einschränkung der Verarbeitung (Art 18)

- Ziel des EU Gesetzgebers?
  - **Personenbezogene Daten dürfen nur mehr gespeichert werden**
  - Keine andere Verarbeitung, es sei denn
    - die Einwilligung des Betroffen liegt vor
    - die Verarbeitung ist für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen notwendig
- Anwendungsfälle
  - **Betroffene** hat die **Richtigkeit bestritten**: für einen Zeitraum, der es dem Verantwortlichen ermöglicht, die Richtigkeit der Daten zu überprüfen;
  - **Datenverwendung ist rechtswidrig**, aber der Betroffene spricht sich gegen Löschung aus und verlangt alternativ Beschränkung;
  - Verantwortlicher benötigt die Daten zwar nicht mehr, aber sie werden **vom Betroffenen zur Geltendmachung, Ausübung oder Abwehr von Rechtsansprüchen benötigt**;
  - Betroffene **widerspricht der Verarbeitung**: für die Dauer der Prüfung kann der Betroffene begehren, dass die Datenverarbeitung eingeschränkt wird

Recht auf Einschränkung der Verarbeitung (Art 18)

- **Gründe für Verweigerung**
  - offenkundig unbegründete Anfrage oder **Exzessivität** (insbesondere im Fall von häufiger Wiederholung; Art 12(5))
- der Verantwortliche unterrichtet den Betroffenen, bevor die Einschränkung aufgehoben wird (Art 18(3))
- **Mitteilungspflicht** des Verantwortlichen
  - Der Verantwortliche informiert jeden Empfänger, dem die personenbezogenen Daten gegenüber offengelegt wurden, über die Einschränkung
    - es sei denn, dies ist unmöglich oder mit unverhältnismäßigem Aufwand verbunden
  - Der Verantwortliche informiert den Betroffenen über diese Empfänger, wenn der Betroffene dies verlangt

Widerspruchsrecht (Art 21)

- Anwendungsfälle
  - Verarbeitung beruht auf berechtigte Interessen (Art 6(1)(f)), einschließlich Profiling; oder
  - Verarbeitung ist für die Erfüllung einer Aufgabe erforderlich, die im öffentlichen Interesse oder in Ausübung der dem Verantwortlichen übertragenen hoheitlichen Befugnisse liegt; oder
  - personenbezogene Daten werden für **Direktmarketingzwecke** verarbeitet
- **Gründe für die Verweigerung**
  - Verantwortliche kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten des Betroffenen überwiegen; oder
  - die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
  - **Wenn sich der Widerspruch auf die Verarbeitung zu Direktmarketingzwecken bezieht: kein Grund zur Verweigerung!**

Widerspruchsrecht (Art 21)

- Bei berechtigtem Widerspruch
  - **Betroffener** ist berechtigt, die Verarbeitung einzuschränken (Art 18(1)(d)) und hat das Recht auf Löschung (Art 17(2)(c))
  - **Verantwortlicher:** keine Verarbeitung von personenbezogenen Daten (Art 21(1) und (3)) und Löschung von personenbezogenen Daten (Art 17(1)(c))

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Novinky

- 3 kategórie OÚ
- Rodné číslo, fotografia, kamerový záznam - ! „bežné OÚ“ !
- GDPR rozlišuje spracovateľskú *operáciu* – **samostatný úkon** s osobnými údajmi (získavanie, uchovávanie, poskytovanie ...) / spracovateľskú *činnosť* – súbor spracovateľských operácií, ktoré sú vykonávané na konkrétny účel spracúvania OÚ
- Dôraz kladený na základné zásady, najmä zásada transparentnosti spracúvania a zásada zodpovednosti prevádzkovateľa

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Časté otázky

Vzťahuje sa GDPR aj na ... ?

Chceme zaviesť kamerový systém, čo ďalej ?

Na akom právnom základe môžem spracúvať fotografie ?

Môžeme na účely dochádzky zaviesť biometriu? Je biometriou aj ... ?

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Vzťahuje sa GDPR aj na ... ?

❖Fyzická osoba

❖Fyzická osoba – podnikateľ

- *Judikatúra ESĽP* (Amann/Švajčiarsko, Niemietz/Nemecko,...)
- *Judikatúra SD EÚ* (Patrick Breyer proti Spolkovej republike Nemecko, Volker und markus Schecke GbR,...)
- *EK (2017)* - Európska komisia zdôrazňuje, že GDPR sa vzťahuje len na fyzické osoby. Ak v členskom štáte fyzická osoba vykonáva ekonomické činnosti, ale podľa vnútroštátneho práva členského štátu nie je považovaná za právnickú osobu, potom by táto osoba mala mať priznanú ochranu podľa GDPR.
- *Oficiálne stanovisko ÚOOÚ SR*

❖! Aj konateľ a kontaktná osoba

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Fotografie zamestnancov

Večierok	Súhlas / OZ ?	IP
Firemný časopis	OZ ?	IP
Intranet	Súhlas / OZ ?	IP
Preukaz	OZ ?	IP

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Chceme zaviesť kamerový systém, čo ďalej ?

Test proporcionality

OZ – ochrana majetku P

Informačná povinnosť (čl. 13/ § 19)

Nerozlišuje priestor prístupný/ neprístupný verejnosti

Záznamy (čl. 30/ § 37)

Zodpovedná osoba ? čl. 37 ods. 1 písm. b) / § 44 ods. 1 písm. b)

Data Breach (čl. 33 + 34/ § 40 + 41)

Bezpečnosť čl. 25, 32, 35 (?)/ § 32, 39, 42 (?)

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Biometria na účely dochádzky

- Čl. 4 bod 14 / § 5 písm. c) – **biometrickými údajmi** sa rozumejú *osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov* týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby *a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu* tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje
- Biometria na účely individuálnej identifikácie fyzickej osoby → **osobitná kategória OÚ**
- Pre použitie : **čl. 9** (podmienky) + **čl. 6** (právny základ)
- § 99 Zákonníka práce – evidencia dochádzky zamestnancov (*biometria nie je upravená* – iný právny základ)
- **Prečo súhlas nie je najvhodnejším riešením ?**
- **Základné zásady spracúvania OÚ**
- Len v ojedinelých prípadoch

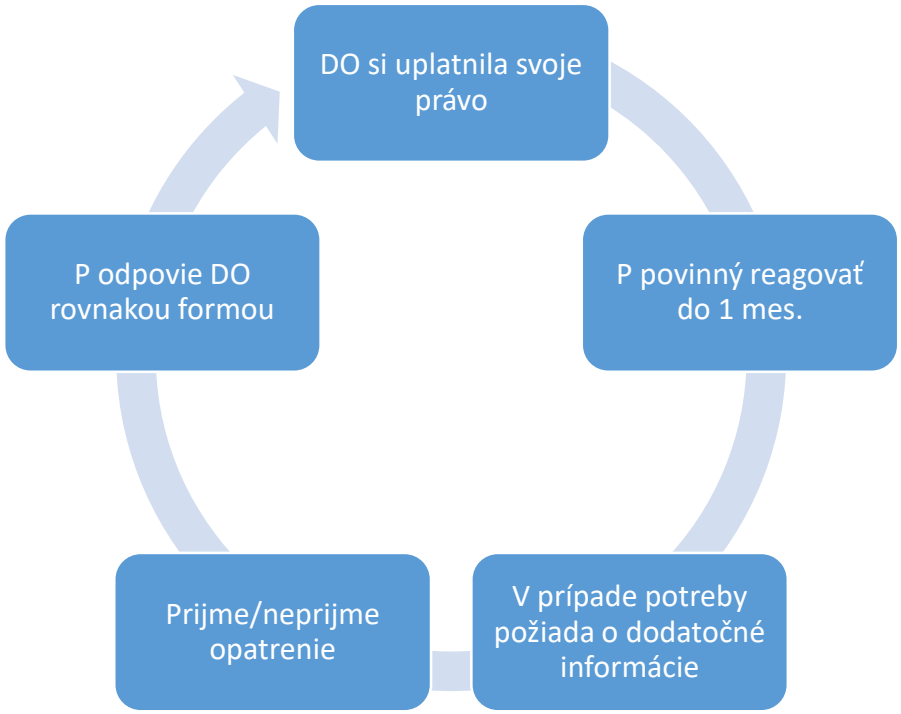
ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Transparentnosť

- **Ústredný princíp** a povinnosť podľa GDPR a zákona
- Odzrkadľuje sa najmä v:
  - informačnej povinnosti prevádzkovateľa
  - komunikácii s dotknutými osobami
  - spôsobe, akým si môžu dotknuté osoby uplatniť svoje práva
- Uplatňuje sa bez ohľadu na použitý právny základ a počas celého spracúvania
- Čl. 12/ § 29 upravuje základné pravidlá uplatňovania tohto princípu
- Informácie alebo komunikácia majú byť:
  - Stručné, transparentné, zrozumiteľné a ľahko dostupné
  - Formulované jasne a jednoducho (s ohľadom na konkrétnu(e) osobu(y)
  - Poskytované písomne alebo inými prostriedkami
  - Bezplatné (! Výnimka čl. 12 ods. 5)

Transparentnosť – vybavovanie žiadostí DO

- Výkon práv dotknutých osôb – **recitál 59**
- Nastavenie **politiky práv** dotknutých osôb
- **1 mesiac** – *možnosť predĺženia*
- Žiadosť o dodatočné info
- môže spoplatniť/ odmietnuť vybaviť, ak je žiadosť opakovaná/ obťažujúca



Aufbewahrungsgrundsätze nach der DSGVO

- **Datenminimierung** (Art 5(1)(c))
  - dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt
  - Prinzip spiegelt sich in Art 25(1) und (2) wieder
    - ErwGr 78: “Datenschutz durch Technik” and “datenschutzfreundliche Voreinstellungen”
    - Auf solche Maßnahmen bezieht sich Art 5(1)(e)
- **Speicherbegrenzung** (Art 5(1)(e))
  - in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist
  - personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten […] ausschließlich für […] **statistische Zwecke** gemäß Artikel 89 Absatz 1 verarbeitet werden

Aufbewahrungsgrundsätze nach der DSGVO

- **Integrität und Vertraulichkeit** (Art 5(1)(f))
  - Verarbeitung, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, **einschließlich Schutz vor** unbefugter oder unrechtmäßiger Verarbeitung und vor **unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung** durch geeignete technische und organisatorische Maßnahmen

Aufbewahrungsfristen – Judikatur

Die Datenschutzbehörde (DSB) hat erst kürzlich in zwei Fällen zur Zulässigkeit der Aufbewahrungsdauer von Daten entschieden:

– GZ: DSB-D216.471/0001-DSB/2018 vom 28.5.2018:
  - Ein Telekommunikationsdienst hat **nach Beendigung des Vertragsverhältnisses weiterhin diverse Daten** (Stammdaten, weitere personenbezogene Daten, Verkehrsdaten) der Beschwerdeführerin gespeichert. Als **Grundlage** für die Aufbewahrung wurden im Wesentlichen die **§§ 132, 207 BAO** angeführt
  - Die Beschwerdeführerin machte die Verletzung des Rechtes auf Geheimhaltung in Folge Speicherung von personenbezogenen Daten über einen gesetzlich zulässigen Zeitraum geltend
  - DSB hat der Beschwerde **stattgegeben** und **aufgetragen** die Speicherung von Stammdaten auf einen Zeitraum von **höchstens sieben Jahren zu beschränken** und Verkehrsdaten sowie personenbezogene Daten (die keine Stammdaten sind) zu **löschen**

Aufbewahrungsfristen – Judikatur

Hierzu führte die DSB im Wesentlichen aus:

- **Unterscheidung** zwischen **gesetzlicher Aufbewahrungsfrist** und **Verjährungsfrist** ist vorzunehmen

- **Aufbewahrung** von Daten ist nur solange erlaubt, wie eine **gesetzliche Aufbewahrungsfrist vorgibt**

- Bei Aufbewahrung der Daten für die Geltendmachung von Rechtsansprüchen: nur wenn die **Aufbewahrung** der Daten durch **ein sich konkret abzeichnendes Verfahren gerechtfertigt** ist. Die bloße Möglichkeit, dass ein Verfahren eingeleitet wird, reicht nicht aus

- Wenn keine besondere gesetzliche Vorschrift für eine Speicherung von personenbezogenen Daten, als für den Zweck, für den sie ermittelt wurden, vorliegen, sind die Daten zu löschen

Aufbewahrungsfristen – Judikatur

Entscheidung der DSB ist aus folgenden Gründen künftig nicht pauschal anzuwenden:

- Anwendbarkeit des Telekommunikationsgesetzes 2003 (TKG 2003)
  - Nach TKG 2003 sind **Stammdaten spätestens nach Beendigung** der vertraglichen Beziehung zu löschen. Ausnahme von der Löschung nach § 97 Abs 2 TKG 2003: ua sonstige **gesetzliche Verpflichtungen**, zB.: Aufbewahrungspflicht nach § 132 BAO (sieht Aufbewahrungsfrist von 7 Jahren vor, außer Daten werden für die Abgabenerhebung betreffende **anhängige** Verfahren benötigt)
- DSB konnte keine besonderen gesetzlichen Vorschriften ermitteln, wonach eine längere Speicherung von Daten erforderlich scheint
- Aussage im Zusammenhang mit Aufbewahrung von Daten für ein sich konkret abzeichnendes Verfahren ist in **Gesamtschau des Falles zu lesen und stellt wohl eine Einzelfallentscheidung dar**

Aufbewahrungsfristen – Judikatur

– GZ: DSB-D123.085/0003-DSB/2018 vom 27.8.2018

- Der Beschwerdeführer hat sich am 17. Mai 2018 sowie am 11. Juni 2018 bei der Beschwerdegegnerin beworben, weshalb personenbezogene Daten des Beschwerdeführers in der Bewerberdatenbank der Beschwerdegegnerin abgespeichert wurden. Der Beschwerdeführer **beantragte** am 31. August 2018 die **Löschung** seiner Daten aus der Bewerberdatenbank
- Die Beschwerdegegnerin teilte mit, dass dem Antrag **nicht entsprochen** wird, da die Bewerberdaten sechs Monate zuzüglich eines Monats für **den potentiellen Klageweg, insgesamt demnach sieben Monate** nach Bewerbungseingang, **gelöscht** werden. Die Bewerberdaten müssen aufgrund eines **potentiellen Verfahrens** nach dem **Gleichbehandlungsgesetz** noch gespeichert werden
- Die DSB **wies die Beschwerde ab**

Aufbewahrungsfristen – Judikatur

– Hierzu führte die DSB im Wesentlichen aus:

- Das Recht auf **Löschung** gemäß (Art 17(1) und (2)) kommt dann **nicht in Betracht**, wenn eine **Verarbeitung** in den von (Art 17(3)(a)bis(e) taxativ aufgezählten Fällen **erforderlich** ist
- Im vorliegenden Fall kam der Tatbestand nach (Art 17(3)(e)) in Betracht: **Verarbeitung der Daten ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich**
- Dabei muss Verantwortlicher darlegen (i) welche **konkreten zukünftigen Verfahren** (ii) auf **welcher Grundlage** anhängig gemacht werden **könnten** und (iii) inwiefern durch derartige Verfahren eine **Notwendigkeit zur weiteren Speicherung** der personenbezogenen Daten begründet wird
- Durch Nennung eines **konkreten Zeitpunktes**, ab wann (Bewerber)daten gelöscht werden, ist für Beschwerdeführer **klar erkennbar**, ab welchem Zeitpunkt seine Bewerberdaten gelöscht werden

Aufbewahrungsfristen und Verjährungsfristen

- **Heranziehung von Verjährungsfristen erforderlich**, **wenn keine gesetzlichen Aufbewahrungsfristen** vorgesehen sind
- DSGVO sieht keine konkreten Fristen für die zulässige Speicherung vor
- Betroffener muss über die Dauer der Speicherung informiert werden. Wenn nicht möglich, muss Verantwortlicher Kriterien für die Festlegung der Speicherfrist bestimmen
- Verjährungsfristen spielen daher große Rolle, va im Arbeits-, und Zivilrecht
- Bei haftungsgeneigten Tätigkeiten ist die Heranziehung von Verjährungsfristen für die Aufbewahrungsdauer gerechtfertigt
  - die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen stellt ein berechtigtes Interesse nach (Art 6(1)(f)) dar

Vor- und Nachteile der Datenaufbewahrung

Vorteile für eine längere Aufbewahrung von Informationen	**Nachteile**
Korrespondenz oder Anweisungen enthalten **Kontaktdaten, die nützlich sein können**	Es ist schwerer, **begrenzte Datenmengen sicher aufzubewahren**
Dokumente oder Aufzeichnungen können bei **Recherchen** wichtig sein	Es ist schwerer**, große personenbezogene Datensätze** im Fall eines Auskunftsersuchens des Betroffenen oder im Fall einer konkreten Suchanfrage (für andere Verarbeitungszwecke) **zu finden**
Dokumente müssen im Falle einer **Reklamation** aufbewahrt werden	Es **steht nicht im Einklang** mit der Verpflichtung zur Einhaltung des **Zweckbindungsgrundsatzes**
Dokumente, Korrespondenz, Rechnungen können zur **Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen** erforderlich sein	Lange Speicherfristen machen es wahrscheinlicher, dass **Datensätze ungenau und veraltet sind**

Erste Schritte zur rechtmäßigen Speicherung der personenbezogenen Daten

- Prüfen Sie die Datensätze, über die Sie bereits verfügen
- Prüfen Sie die Dauer, für die Sie diese Datensätze speichern
- Berücksichtigen Sie, für welchen Zweck Sie die Daten aufbewahren, um zu entscheiden, ob (und wie lange) die Daten aufbewahrt werden sollen
- Löschen Sie Daten, die Sie für diesen Zweck oder diese Zwecke nicht mehr benötigen
- Aktualisierung, Archivierung, Anonymisierung oder Löschung von Datensätzen, wenn sie veraltet sind

Erstellung einer Löschpolicy

- Löschpolicy spiegelt die Erkenntnisse wieder (siehe vorherige Folie)
- Beurteilung der tatsächlich gelebten Compliance mit der Löschpolicy und Anpassung bei Bedarf
- Löschpolicy sollte einheitliche Aufbewahrungsfristen für bestimmte Datenkategorien enthalten
- Grundlage für die Entscheidung, wie lange personenbezogene Daten aufbewahrt werden
  - Verarbeitungszweck
  - Geschäftliche Notwendigkeit
  - Nationale Rechtsvorschriften

Überblick über die Aufbewahrungsfristen nach slowakischem Recht

Verzeichnis von Verarbeitungstätigkeiten

- jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen (Art 30(1)); - dies gilt für den Auftragsverarbeiter ggf. sein Vertreter;
- der Verantwortliche darf sein eigenes Verzeichnis erstellen, gegebenfalls darf er durch das Amt das veröffentlichte Musterverzeichnis benutzen; in jedem Fall muss das Verzeichnis die erforderlichen Bestandsteile aufweisen (Art. 30(1) a.) bis g.) und Art. 37 des slowakischen Datenschutzgesetzes);
- einer der Bestandteile des Verzeichnises ist die Festlegung der vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien – d.h. die Festlegung der Aufbewahrungsfristen für verschiedene Datenkategorien;
- bei Erstellung des Verzeichnises für die Klienten gehen wir von den durch das Amt vorgesehenen Aufbewahrungsfristen aus;

Die Ausnahme von der Pflicht zur Erstellung der Verzeichnises von Verarbeitungstätigkeiten

- Ein Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen **und**

- die von ihren vorgenommenen Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt;

- die Verarbeitung erfolgt nicht nur gelegentlich oder

- die Verarbeitung weder besonderer Datenkategorien gemäß Art. 9 (1) der DSGVO / Art. 16 des Gesetzes (z.B. biometrische Daten), noch personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 der DSGVO / Art. 17 des Gesetzes wird nicht eingeschlossen;

Arbeitnehmerdaten – empfohlene Aufbewahrungsfristen

Datenkategorie/ Dokument	Empfohlene Aufbewahrungsfrist	Beginn der Aufbewahrung
Personalauswahl (personenbezogene Daten angegeben im Lebenslauf, Bewerbungsschreiben, Fragenbogen, im Dokument über abgeschlossene Ausbildung)	6 Monate	Ab Ende der Ausschreibung
Personalistik (Personalakte, die hauptsächlich das Arbeitsverhältnis betreffen, Personalfragebogen, Dokumente und Bestätigungen, die der Arbeitsgeber erfordert und andere Dokumente betreffend Entstehung, Verlauf und Ende des Arbeitsverhältnisses)	70 Jahre	Ab Ende des Arbeitsverhältnisses
Gehaltspolitik des Arbeitsgebers (übliche persönliche Angaben, Gehalt, Lohn oder Lohnverhältnisse und weitere finanzielle Angelegenheiten, Stundenlistendaten, Daten über wichtige persönliche Hindernisse in der Arbeit, Angaben über die veränderte Arbeitsfähigkeit usw.)	50 Jahre	Ab Ende des Arbeitsverhältnisses

Arbeitnehmerdaten – empfohlene Aufbewahrungsfristen

Datenkategorie/ Dokument	Empfohlene Aufbewahrungfrist	Beginn der Aufbewahrung
Arbeitszeiterfassung (Personendaten, Daten über die geleistete Arbeitszeit, Daten über die Arbeitsunfähigkeit, über wichtige persönliche Hindernisse in der Arbeit, Arbeitseinordnung, Daten über Familienangehörige usw.)	10 Jahre	Ab Ende des Arbeitsverhältnisses
Pflichterfüllung des Arbeitsgebers gegenüber der Krankenkasse (übliche Personendaten, Geburtsnummer, Daten betreffend Gesundheit)	10 Jahre	Ab Ende des Kalenderjahres, auf das sich die Informationen beziehen
Pflichterfüllung des Arbeitsgebers gegenüber der Sozialversicherung (übliche Personendaten, Daten über die Pensionsanerkennung, Daten über den Karenzurlaub, Elternurlaub)	10 Jahre	Ab Ende des Kalenderjahres, auf das sich die Informationen beziehen

Arbeitnehmerdaten – empfohlene Aufbewahrungsfristen

Datenkategorie/ Dokument	Empfohlene Aufbewahrungsfrist	Beginn der Aufbewahrung
Pflichterfüllung des Arbeitsgebers im Bereich der Sicherheit und Gesundheitsschutz bei der Arbeit (übliche Personendaten, Geburtsnummer, Daten betreffend Gesundheit)	5 Jahre	Ab Ende bzw. Erlöschung der Pflicht
Erfüllung der Steuerpflicht des Arbeitsgebers (übliche Personendaten, Geburtsdatum, Geburtsnummer, Kontonummer und Einkommensdaten)	10 Jahre	Ab Ende des Kalenderjahres, auf das sich die Informationen beziehen
Einführung der Kontrollmechanismen durch Überwachung nach dem Arbeitsgesetzbuch (übliche Personendaten – Kameraaufzeichnungen, Daten aus den Identitätnachweisen (Personalausweise), Überwachung der Telekommunikation von den Telefonnummern des Arbeitnehmers)	15 Tage 5 Jahre	Ab Erstellung der Kameraaufzeichnungen Ab Erstellung der ID-Ausweisaufzeichnungen

Arbeitnehmerdaten – empfohlene Aufbewahrungsfristen

Datenkategorie/ Dokument	Empfohlene Aufbewahrungsfrist	Beginn der Aufbewahrung
Kopieren von amtlichen Dokumenten (Personendaten im Umfang der kopierten amtlichen Dokumenten)	Steuerunterlagen – 10 Jahre Restliche Dokumente – 3 Jahre	Ab Ende des Jahres, auf das sich die Informationen beziehen Ab Ende des Arbeitsverhältnisses
Exekution (Identifizierungs- und Kontaktdaten, Daten in den Benachrichtigungen über Exekutionsbeginn, im Bericht über Exekutionszustand, in der Arrestanordnung)	10 Jahre	Ab Ende des Kalenderjahres, auf das sich die Informationen beziehen
Buchhaltungsunterlagen	10 Jahre	Ab Ende des Kalenderjahres, auf das sich die Informationen beziehen oder ab dem Moment der Verwendung der Buchhaltungsdaten.

Daten anderer Personen als Arbeitnehmer – empfohlene Aufbewahrungsfristen

Datenkategorie/ Dokument	Empfohlene Aufbewahrungsfrist	Beginn der Aufbewahrung
Evidenzführung der Eintritte in die Räumlichkeiten des Betreibers (Vorname, Nachname, Ausweisnummer, Zeit des Ankommens und Weggehens, besuchte Person, Unterschrift usw.) / Besuche, natürliche Personen eintretende in die Räumlichkeiten des Betreibers	1 Jahr	Ab Ende des Kalenderjahres, im dem sich der Eintritt stattfand
Überwachung der Räumlichkeiten zum Zweck des Besitzschutzes und der Gesundheit (Aufzeichnung aus der Kameravorrichtung) / natürliche Person aufgezeichnet auf der Aufnahme aus der Kameravorrichtung	15 Tage	Nach der Erstellung der Aufzeichnung
Geschäftskommunikation (übliche Personendaten, insb. Identifikations- und Kontaktdaten) / Lieferanten, Abnehmer und ihre Mitarbeiter	5 Jahre	Ab Ende des Kalenderjahres, in dem die Kommunikation beendet wurde

Bezpečnosť osobných údajov

- **Špecificky navrhnutá a štandardná ochrana OÚ** – zohľadniť najnovšie poznatky, náklady na vykonanie opatrení, rozsah, kontext a účely spracúvania OÚ, pravdepodobné riziká a ich závažnosť vo vzťahu k právam DO; prijatie primeraných BO (čl. 25/§ 32)
- **Bezpečnosť podľa čl. 32/§ 39** – analýza rizík vo vzťahu k spracovateľskej činnosti P, prijatie primeraných BO, snaha o elimináciu vysokého rizika, povinnosti pre P aj S
- **Posúdenie vplyvu** – podmienky stanovené v čl. 35/§ 42, konkrétna spracovateľská operácia; stanovená požiadavka na minimálny obsah bezpečnostnej dokumentácie; postup pri posúdení vplyvu upravený vyhláškou; pri zmene aktualizovať
- **Predchádzajúca konzultácia** – povinnosť P ešte pred spracúvaním OÚ požiadať úrad o predchádzajúcu konzultáciu, ak výsledkom posúdenia vplyvu bolo vysoké riziko na práva DO a P neprijal opatrenia na zmiernenie tohto rizika

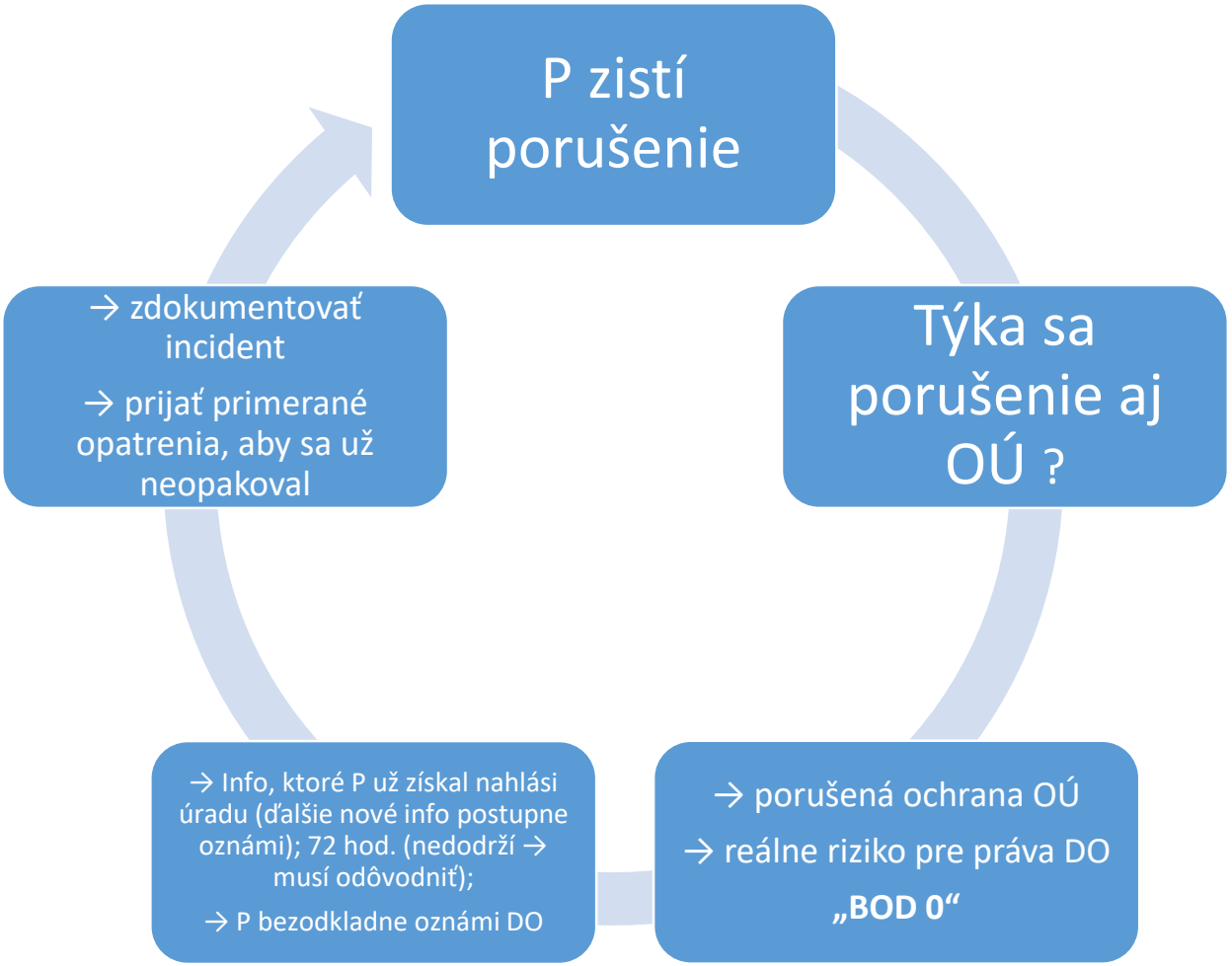
ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Oznámenie porušenia OÚ

- nástroj zlepšujúci súlad v súvislosti s ochranou OÚ
- naplánovať a zaviesť postupy na odhalenie porušenia a rýchle zabránenie jeho šíreniu, posúdenie rizika pre jednotlivcov a určenie či je potrebné informovať úrad a DO
- typ bezpečnostného incidentu – ***všetky porušenia ochrany OÚ sú bezpečnostnými incidentmi***, *NIE všetky bezpečnostné incidenty sú porušeniami ochrany OÚ*

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Postup pri bezpečnostnom incidente



Postup pri porušení ochrany OÚ

Kedy dochádza k porušeniu ochrany ?

Kedy mi začína plynúť lehota ?

Čo a ako mám úradu oznámiť ?

Mám to oznámiť aj DO ?
Dokedy a ako ?

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Kedy dochádza k porušeniu ochrany ?

- Definícia porušenia ochrany - čl. 4 (12)/§ 5 písm. m)
- P musí vedieť najskôr porušenie identifikovať (*napr. zničenie, strata, zmena, neoprávnený prístup a pod.)*
- *Typy porušenia ochrany OÚ*
  - ✓ *Porušenie dôvernosti (neoprávnené/náhodné poskytnutie OÚ/ prístupu k OÚ)*
  - ✓ *Porušenie integrity (neoprávnená/náhodná zmena OÚ)*
  - ✓ *Porušenie dostupnosti (neoprávnená/náhodná strata prístupu/ zničenie OÚ)*

✓ Porušenie	✖ Nie je porušenie
dočasná strata dostupnosti (výpadok el. prúdu/ útok)	Plánovaná údržba systému (dočasná strata dostupnosti)

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Čo, ako a v akej lehote mám úradu a DO oznámiť ?

	Lehota	Ako	Čo	V akom prípade
ÚOOÚ SR	→ Do 72 hod. → od kedy sa „dozvie“ = primeraná úroveň istoty	Formulár zverejnený úradom	→ čo sa stalo → povaha OÚ → počet DO → KÚ ZO → prav. následky → opatrenia	Porušenie pravdepodobne povedie k riziku pre práva a slobody DO, napr.: → e-mail s priamym marketingom je odoslaný viacerým príjemcom v kolónke „komu“ → banka odoslala výpis z účtu nesprávnemu príjemcovi → v dôsledku kybernetického útoku došlo k strate OÚ ❖ **Porušenie s nízkym rizikom**
DO	Bezodkladne (môže nariadiť aj úrad)	→Špecializ. správy → sms, e-mail, oznámenia na webovom sídle → médiá → kombinácia → vhodným jazykom	→ čo sa stalo → povaha OÚ → počet DO → KÚ ZO → prav. následky → opatrenia	Porušenie pravdepodobne povedie k vysokému riziku pre práva a slobody DO, napr.: → v dôsledku kybernetického útoku sa útočník dostane k prihlasovacím menám a heslám DO do ich účtov → nemocnica dočasne stratí prístup k zdravotným záznamom ❖ **Porušenie s vysokým rizikom**

Ihre Ansprechpartner im Datenschutzrecht bei CMS

JUDr. Jozef Čupa, LL.M.
Senior Associate
CMS Slovakia
T +421 2 3214 1414
E jozef.cupa@cms-rrh.com

Dr. Johannes Juranek
Partner, Technology
CMS Austria & CEE
T +43 1 40443 2450
E johannes.juranek@cms-rrh.com

Mag. Peter Šimo
Partner
CMS Slovakia
T +421 2 3214 1414
E peter.simo@cms-rrh.com